(2)

PERSEREC

PERS-TR-92-007
JUNE 1992

Security Awareness Training And Education (SATE): A Survey Of DOD Installations

Joseph P. Parker
BDM International, Inc.

James A. Riedel
Defense Personnel Security Research Center

Martin F. Wiskoff
BDM International, Inc.

Approved for Public Distribution:
Distribution Unlimited

Defense Personnel Security Research Center
99 Pacific Street, Building 455-E
Monterey, CA 93940-2481

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION AVAILABILITY OF REPORT
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) PERS-TR-92-007	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION BDM Corporation, Inc. — 6b OFFICE SYMBOL (If applicable)	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code) 2600 Garden Road, Suite 230 Monterey, CA 93940	7b ADDRESS (City, State, and ZIP Code)
8a NAME OF FUNDING SPONSORING ORGANIZATION Defense Personnel Security Research Center (PERSEREC) — 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code) 99 Pacific St., Bldg. 455-E Monterey, CA 93940-2481	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO — PROJECT NO — TASK NO — WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
Security Awareness Training and Education (SATE): A Survey of DoD Installations

12 PERSONAL AUTHOR(S)
Parker, J. P., Riedel, J. A., & Wiskoff, M. F.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Technical	FROM _____ TO _____	1992 June	79

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Security awareness; Security education; Personnel security; Information security; Security briefing; SATE

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This report presents the results of a survey designed to describe the shape of current Security Awareness Training and Education (SATE) programs in DoD, focusing on the military services. Overall, the security representatives who were interviewed rated their SATE programs as moderately successful. However, five areas are identified where modest changes could improve the effectiveness of such programs. They are: instructional media enhancements, security manager training, SATE policy and requirements, security manager support, and security inspections. Recommendations in each of the five areas are presented.

20 DISTRIBUTION AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL ROGER P. DENK, Director	22b TELEPHONE (Include Area Code) (408) 646-2448 — 22c OFFICE SYMBOL

DD Form 1473, JUN 86 — Previous editions are obsolete — SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603

PERS-TR-92-007 June 1992

SECURITY AWARENESS TRAINING AND EDUCATION (SATE): A SURVEY OF DOD INSTALLATIONS

Joseph P. Parker
BDM International, Inc.

James A. Riedel
Defense Personnel Security Research Center

Martin F. Wiskoff
BDM International, Inc.

The work contained in this report was funded under
Purchase Order N00014-87-D-0715-3006

Defense Personnel Security Research Center
99 Pacific Street, Building 455-E
Monterey, California 93940-2481

PREFACE

An integral and mandatory part of the Department of Defense (DoD) security program involves educating cleared personnel concerning their individual responsibilities for safeguarding classified information and the possible grave consequences of failing to protect the nation's secrets. It is unknown what impact this security awareness education has on individual security knowledge, attitudes, and behavior, though it is generally accepted that these programs are critical to the protection of the nation's secrets.

Concerns have been expressed in recent congressional hearings and testimony with regard to the effectiveness and efficiency of security awareness programs in the DoD. In formulating the research agenda for the Defense Personnel Security Research Center (PERSEREC), several DoD components stressed the need for research directed toward the improvement of security awareness training and education (SATE).

This research presents the results of a survey designed to describe the shape of current SATE programs in DoD. This report details many of the problems facing the individuals responsible for carrying out such programs and suggests areas in which modest changes could make a large difference in the effectiveness of such programs.

The authors would like to thank the organizations and individuals who provided valuable assistance in the preparation of this report. Security personnel at each of the participating installations gave generously and willingly of their time, as did officials in several government security organizations and agencies. Our thanks also go to Ernie Haag of HumRRO for help in the survey design and data collection, to Suzanne Wood of PERSEREC for background research, and to Lynn Fischer of the Department of Defense Security Institute (DoDSI) for his review of the survey instrument and report.

PERS-TR-92-007 June 1992

SECURITY AWARENESS TRAINING AND EDUCATION (SATE): A SURVEY OF DOD INSTALLATIONS

EXECUTIVE SUMMARY

Joseph P. Parker
James A. Riedel
Martin F. Wiskoff

Background

Since 1985 a number of reports have been issued by commissions and Congressional committees in which recommendations to improve security awareness training and education (SATE) in government have been proposed. In response, offices within the Department of Defense (DoD) and the Military Services have indicated the need to increase our knowledge of how SATE programs are being conducted and to assess their strengths and weaknesses as a prerequisite to introducing improvements.

Objectives

The present study seeks to obtain information concerning the state of security awareness training and education at Service installations. Specifically, the study attempts to determine:

1. the amount and adequacy of the time devoted to the coverage of various security topics and disciplines;

2. the quality and availability of media and training methods used in SATE;

3. the level of compliance with SATE regulations, the mechanisms that are in place to ensure compliance, and indicators of program effectiveness;

4. the level of support for SATE expressed in command emphasis, personnel and funding resources, and general receptivity;

5. the adequacy of regulations which govern SATE at different levels;

6. the adequacy of security staff training and development and the training sources and methods that are used;

7. the current and potential effectiveness of specific SATE program components.

Methodology

Planning for the survey project was initiated by meetings with Service headquarters representatives and installation security staff members involved in information and personnel security. Information concerning SATE programs and recommendations for their improvement was obtained in these meetings.

On the basis of these discussions, two survey forms were constructed. The first was a detailed interview protocol which contained a mix of closed questions (*e.g.*, yes/no, multiple choice, and rating items) and open-ended questions. The second form was a 100-item questionnaire comprised almost entirely of rating items.

Data were collected between July and October 1990 at a total of 58 sites (18 Army, 12 Navy, 23 Air Force, 4 Marine Corps and one DoD). At each site a researcher interviewed the installation security office representative for approximately 2 1/2 hours using the structured survey form. The second form was also completed by the interviewee. Meetings were also held with small numbers of unit security representatives and/or security staff at which time only the second survey form was completed.

Survey data were received from a total of 111 individuals. Forty-seven security office representatives completed the interview form and all but seven of these also completed the questionnaire. Sixty-four unit security representatives--mostly unit security managers--completed only the questionnaire. A total of 104 questionnaire forms and 47 interview forms were completed.

Findings

Findings addressing each of the areas specified in the objectives are presented in the report. Overall, security managers rated their SATE programs as moderately successful. They felt that they had provided personnel with the required security indoctrinations and had positively contributed to the security inspection and review process.

However, two primary areas were identified where additional assistance to the security manager could improve SATE programs:

1. Security professionals repeatedly expressed concern with the limited availability and poor quality of media products. Lack of a reliable, timely, and sufficiently comprehensive distribution system also prevented them from acquiring more commonly available SATE publications and materials.

2. Newly assigned unit security managers lacked appropriate experience or training in their positions. Training opportunities were not readily accessible due to the location of the training, limited class sizes and difficulty in attending training away from the work site.

Three other areas were mentioned where lesser, but nonetheless important, improvements could be made to SATE effectiveness:

3. The existence of multiple Service and local regulations caused difficulty because the requirements for security education in various disciplines are presented separately. Computer and communications security regulations were frequently singled out as difficult to use because the language presupposed a level of technological knowledge that many security personnel did not possess.

4. Few commanders or others in leadership positions were visible in security awareness training activities, nor did they provide effective mechanisms for enabling the security manager to enforce participation in security programs.

5. Managers felt that security inspections focus on documenting compliance with requirements, *e.g.*, reports of security violations and training attendance records, rather than on the impact of the programs on the cleared population.

Recommendations

The following recommendations for improvements to SATE programs in DoD correspond to the five areas presented above:

1. Create a centralized distribution system for SATE materials that would be easily accessible to security managers. This would entail establishing an office responsible for acquiring and disseminating security materials. The Department of Defense Security Institute is currently in the early planning phases of providing this service to DoD components. An additional need that could be performed by the clearinghouse is improving the quality of such security awareness materials as posters, videotapes, pamphlets and newsletters.

2. Bring training to the security manager by means of correspondence courses or mobile SATE training teams. In addition, training could be conducted at regional locations where requirements for travel could be minimized. Particular attention should be paid to the rapidly emerging security needs in the computer and communications areas.

3. Consideration should be given to simplifying and/or reducing the number of regulations and supplements relevant to security education. This effort could be initiated at the DoD level, perhaps as a special task group made up of Office of the Secretary of Defense, Service headquarters and field representatives. Guidance could be provided and procedures established for improving the translation of Service SATE regulations into local regulations.

4. Structure SATE programs to involve commanders and senior staff. In addition, provide better indoctrination and continuing reminders to superiors concerning the role and importance of SATE to their organization's security.

5. Develop better tools and instruments for assessing the effectiveness of SATE programs at the unit and installation levels. Structure security inspections to be assistance-oriented, whereby helpful feedback is provided to security managers during and after inspections.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Background

The need to improve security awareness training and education (SATE) surfaced in a 1985 report from the Stilwell Commission (DoD Security Review Commission) which had been tasked to review DoD security policies and practices. The Commission noted that all DoD components with classified functions had some type of security awareness program, "consisting typically of required briefings, briefings statements, audiovisual aids, posters, and publications of all types, describing the hostile intelligence threat" (p. 69). The Commission described these programs as having been "reasonably effective in sensitizing personnel to possible hostile intelligence approaches" (p. 69). However, the report suggested that DoD could avoid some duplication of effort and improve the quality of briefings and training aids by better coordinating and facilitating its programs.

In January 1986 the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs issued a report (United States Senate, 1986) that concluded:

> Continuing security awareness programs on behalf of federal agencies and industrial contractors should be given the highest priority. These programs should emphasize the harsh realities and grave personal consequences of espionage in an attempt to dispel popular misconceptions of espionage as an often glamorous and intriguing adventure (p. 20).

In October 1988, the House of Representatives published *U.S. Counterintelligence and Security Concerns: A Status Report. Personnel and Information Security.* This report was produced by the Subcommittee on Oversight and Evaluation of the Permanent Select Committee on Intelligence and was a follow-up to their 1986 report on counterintelligence and security. The need to improve security awareness had been a concern of the 1986 report, and the 1988 report pointed out continuing gaps in this area. "Not enough is done," the Committee wrote, "to promote security awareness."

> The Pollard case demonstrated the great value of security awareness by fellow employees as a tipoff to possible espionage. Some recent espionage cases also raise the possibility that U.S. intelligence should have picked up clues that something was amiss and taken appropriate action (p.4).

While strong agreement appears to exist on the essential nature of SATE programs to national security, no systematic effort, with one exception (Bosshardt, DuBois, and Crawford, 1991a), has been made to determine the major needs and problems of individuals charged with carrying out SATE programs.

Overview of SATE Requirements

Security awareness training and education activities in the DoD are driven by requirements that flow down from Presidential directives and Executive Orders to agency or departmental regulations. These regulations guide and shape the SATE programs at installations such as those that took part in the survey. Security training and education for individuals with collateral (Confidential, Secret and Top Secret) clearances and those with sensitive compartmented information (SCI) access are regulated by two different groups of requirements.

The principle DoD regulations that direct security education for individuals with collateral clearances are the *5200.1-R Information Security Program Regulation* and the *5200.2-R Personnel Security Program Regulation*. In implementing these two regulations at the Service level, the Army and Air Force have each produced two sets of regulations which mirror the 5200.1-R and 5200.2-R on security education, while the Navy has produced a single document which covers both information and personnel security.

The principal unclassified regulation guiding security education in the intelligence community is the *DCID 1/14 Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*. The minimum standards for SCI security awareness programs are detailed in Annex C of the DCID 1/14. (A more complete description of the regulations pertinent to SATE is provided in Appendix A.)

Overall, the Service and agency requirements for security education at both the collateral and SCI clearance levels are similar and primarily consist of five different types of briefings: initial, refresher, foreign travel, counterintelligence, and termination. These briefings form the heart of SATE programs and were, as such, a major focus of this research.

Separate DoD regulations governing physical security, operations security, communications security, and automated information systems (AIS) security also exist, and mandate security education in the corresponding discipline, but only in the information and personnel security regulations are the general form of the security education program as a whole described in substantive detail.

In addition to the cascading regulations mentioned, local regulations concerning security education in the form of training manuals, pamphlets, supplements, handbooks, *etc.*, form an important part of the security program at many installations.

Objectives

The present research obtained information concerning the current state of SATE at Service installations. Specifically, the research:

1. assessed the amount and adequacy of the time devoted to the coverage of various security topics (safeguarding, authorized access, accountability, espionage threat, communication & transmission, and others) and security disciplines (information, personnel, industrial, physical, operations, communications, AIS, and others);

2. assessed what types of media and training methods are being used in carrying out security education activities, evaluated their quality and availability, and described the sources for such materials;

3. assessed the level of compliance with SATE regulations, ascertained what mechanisms are in place to ensure or enhance compliance, and reviewed any indicators of program effectiveness;

4. determined the level of support for SATE expressed in command emphasis, personnel and funding resources, and general receptivity;

5. evaluated the adequacy of regulations which govern SATE at different levels;

6. described what type of security staff training and development is taking place and detailed what training sources and methods are used; and

7. assessed the current and potential effectiveness of specific SATE program components.

METHODOLOGY

Preliminary Interviews

Headquarters

The initial step in the project entailed meeting with headquarters representatives from the Army, Navy and Air Force. Since security awareness programs are usually the responsibility of information and personnel security officers and managers, conversations were principally held with individuals in those offices. During these meetings information concerning the objectives and operation of Service SATE programs was obtained, along with recommendations for their improvement. Discussions were also held with staff in the office of the Deputy Under Secretary of Defense for Security Policy[1], the Department of Defense Security Institute (DoDSI), and the Information Security Oversight Office.

Field Sites

Interviews with installation security staff members were held at 10 military installations (four Army, two Air Force, and four Navy). The purpose of these initial interviews was to: (1) obtain a preliminary understanding of the objectives and operation of Service branch SATE programs, (2) gather the information necessary for developing a research approach, and (3) obtain recommendations for the improvement of SATE programs.

A semi-structured interview protocol was used to obtain information concerning various aspects of SATE. Topic areas included policy guidance, instructional content and methods, availability of instructional products, management support, resources, security staff training and development, program effectiveness, and recommendations for improving SATE programs.

The interview results suggested that data should be gathered from installation security office representatives and unit security representatives for the survey. The results also pointed to the value of sampling organizations varying in terms of size, mission, echelon, amount of classified holdings, and geographic location. These interviews provided considerable information regarding operation of SATE programs in

[1]As a result of a reorganization within the Office of Defense in FY91, SATE policy is currently promulgated by the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures) (DASD[CI&SCM]), Command, Control, Communications and Intelligence (C3I).

the military branches and identified program impediments and suggestions for improvement.

Development of Survey Forms

Two survey forms were developed based on the results of the initial series of site visits. The first was a detailed interview protocol combining both closed and open-ended questions. Closed questions were included to enable more precise measurement of interview responses and to facilitate statistical analyses. The types of questions included yes/no, multiple choice, and rating items. Within the rating items group, different scoring and scaling techniques were used depending on the question. In some instances, interviewees were presented with a list (*e.g.*, media products, training methods, SATE regulations) and asked to rank-order list elements according to their usefulness, frequency of use, availability, or other criteria. In other instances, interviewees were presented with statements or elements of a list and asked to rate each on a numerical scale provided. Each point on the scale would correspond with a descriptive expression. For example, the five points on a scale measuring frequency of use for training media correspond to the terms *never, seldom, sometimes, often,* and *always*. Numerical rating scales were used throughout the interview form to measure dimensions such as the adequacy of SATE regulations, the quality and availability of professional training courses, and the usefuiness of SATE products.

Questions of an open format often followed direct Yes/No questions such as, "Do local SATE regulations need to be improved?" In this example, interviewees who responded yes were then asked to explain in their own words what improvements they considered most important. Open-ended questions were also used as a follow-up to multiple-choice or rating items. This approach allowed respondents to describe a broad range of problems and possible improvements and discuss them in depth.

The second form was a 100-item questionnaire comprised almost entirely of less time-consuming rating items. It was developed to aid in quantifying the relative importance and magnitude of various SATE impediments and to increase the precision and reproducibility of the results. Respondents were presented with statements phrased as problems and asked to rate each according to how much of an obstacle it was to maintaining a highly effective SATE program. A 10-point rating scale was used for all problem items. Verbal descriptions used to identify scale positions included *no problem, minor problem, moderate problem,* and *major problem*. Most of the content areas addressed in the interview form were also covered in the questionnaire. Content areas covered in the forms are presented in Table 1.

Table 1

Content Areas Covered in Survey Forms

Respondent Information - pay grade, years of experience in security, and position tenure.

Organizational and policy information - the size and primary mission of installation; size of security office; amount of time spent by security staff on SATE activities; DOD, Service, and local policies governing SATE activities.

SATE Practices - the SATE time spent covering various security topics and disciplines, staff expertise in specific subject matter and disciplines, SATE objectives, use of media and training methods, and sources for SATE media and products.

Program Management - internal and external support for SATE implementation, accountability, security awareness in performance appraisals, security inspections, security office controls, program emphasis at different organizational levels, security staff training and development, and effectiveness of SATE programs.

Survey Data Collection Procedures

An attempt was made to survey a cross-section of DoD sites including Air Force, Army, Navy, and Marine Corps installations. Within each Service, installations varying in size, mission, type of access required, proportion of civilian to military personnel, and geographic location were sampled. The goal was to balance the sample in terms of these attributes.

A decision was made against trying to obtain a sample of organizations large enough to determine whether SATE practices or impediments differed at installations based on the above characteristics. This was done for three reasons. First, the survey's goal was to identify impediments to effective SATE and potential remedial actions rather than to precisely determine the perceived magnitude of various problems across different types of organizations. Second, related research (Bosshardt et al., 1991a) found few substantive differences in security education between organizations based on Service branch, access level, or whether they were predominantly military or civilian. Therefore, there was little reason to expect systematic differences. Third, a representative sample large enough to test for differences among these organizational groupings would have required a much larger investment of resources given our use of time-consuming, open-ended questions in the interview protocol.

Given the sampling design limitations discussed above, we still feel that the impediments and areas of success identified in this report are reasonably representative of those to be found in the armed Services and much of DoD. This assertion is supported by our finding that results generalized across the Services and across installations varying in several key attributes.

At each site a researcher interviewed the installation security office representative using the interview form. This interview lasted approximately 2 1/2 hours. Interviewees were also asked to complete the questionnaire. Whenever possible, the researcher also conducted a separate 1-hour meeting with a small number of unit security representatives and/or security staff. During these group meetings, the researcher had participants independently complete the questionnaire. A discussion of SATE issues generally followed completion of the survey forms.

Description of the Survey Samples

Descriptive information was gathered regarding several characteristics of the survey sample including site characteristics, respondent characteristics, clearance information, and time spent on SATE activities by security staff members.

Site characteristics

Survey data were collected from a total of 58 sites. A complete list of participating sites is shown in Appendix B. The sample includes 18 Army, 12 Navy, 23 Air Force, and 4 Marine Corps sites, along with one DoD facility. At 73% of these sites the military personnel outnumbered civilian personnel, while at 27% of the sites the opposite was true. The primary mission of the organizations and their proportion of the total sample were as follows: tactical/strategic 32%, training 28%, logistics/support 26%, scientific/research and development 10%, intelligence 9%, and other 5%.

Respondent characteristics

Survey data were received from a total of 111 individuals. Forty-seven installation security office representatives completed the interview protocol and all but seven of these also completed the questionnaire. Sixty-four unit security representatives--mostly unit security managers--completed only the questionnaire, bringing a total of 104 questionnaire forms and 47 interview protocols completed.

Installation security office representatives, who will henceforth be referred to as interviewees, had an average 17 years of experience in security, had spent nearly five years in their current position, and had been employed at their current installation for

slightly over seven years on average. Overall, the interviewees could be characterized as having a great deal of experience in their positions. Respondent data were not collected from the unit security representatives who completed only the questionnaire.

Clearance information

The ratio of cleared to uncleared personnel across all sites was approximately four to one, and at only two of the sites did uncleared personnel outnumber those with clearances. Personnel with collateral clearances outnumbered those with SCI-level access at 47 of the sites; at the remaining 11 sites the opposite was true.

Security staff time expended on SATE

Installation representatives reported having an average of eight personnel on their security staff. The mean number of security staff assigned some responsibility for designing or delivering SATE was slightly more than three. On average, interviewees spent 88% of their time on security-related activities. Nearly 28% of that time was spent by interviewees and their immediate security staff in the design and delivery of security awareness training and education activities.

The average number of unit security managers supported by the installation security office was 24. On average, 35% of the unit security manager's time was spent on security activities. This low number reflects the fact that the unit security manager position is a part-time duty for most individuals. Only 33% of their time spent on security activities was dedicated to the design and delivery of SATE activities. This equates to approximately 12% of the unit security manager's total time being devoted to SATE.

Data Reduction and Manipulation

Responses to Yes/No, multiple choice, and limited choice questions were converted to numerical data and automated. All open-ended responses were typed verbatim into a data retrieval system and printed out by item number in a non-coded format.

All 10-point rating scales were collapsed into four groupings corresponding to the four verbal descriptions provided for each rating continuum. However, in calculating mean scores for these rating items the full scale was used to obtain more precise estimates. Summary variables were also created in some instances to enable comparisons of results by content and subject areas.

Open-ended responses were placed into inductively derived categories and the number of responses tabulated. These derived categories frequently resembled subject areas identified in the taxonomy of the interview protocol.

RESULTS

Introduction

The results section is presented in eight subsections covering the areas of inquiry listed below, which roughly correspond to the seven stated objectives of the report. This format is similar to the structure of the Interview Form used, though not all questions covering a given subject area were necessarily grouped together in this manner on the form.

1. Security Awareness Objectives and Subject Matter Coverage
2. Training/Education Methods and Media Products
3. Accountability
4. Emphasis and Support for Security Awareness
5. Security Awareness Training and Education Regulations
6. Training for Security Personnel
7. SATE Effectiveness
8. Other Survey Topics

At the beginning of each of the eight subsections, excepting the last, a summary of the results for that subsection is presented.

Security Awareness Objectives and Subject Matter Coverage

Summary

Convincing employees that compliance with security regulations is essential to national security was considered an extremely important and not overly difficult objective to achieve. Yet it was quite difficult to convince employees to report on coworkers who violate these security rules. Respondents indicated that the average cleared employee spends approximately 7 hours annually in SATE briefings and meetings, and that slightly more time needs to be devoted. Of the various SATE topics covered in indoctrination and refresher briefings, the largest amount of time was devoted to physical safeguarding of classified information, followed by the espionage threat. Among the security disciplines, information and personnel security received the most time whereas computer security was seen as the least adequately covered. This shortfall was primarily due to a lack of technological expertise required to comprehend and address this area, but cumbersome, difficult-to-understand computer security requirements were also blamed.

Objectives

Interviewees were presented with the six SATE objectives listed below and asked to identify what they considered to be the single most important among them. Most of these objectives can be found stated in similar terms in the SATE regulations previously cited. Others were developed by the authors and are based on preliminary interviews and conversations. The list is not intended to be exhaustive.

1. Implant the belief that compliance with security rules and regulations really has a positive impact on national security.

2. Demonstrate and convince personnel that past instances of espionage have damaged national security.

3. Convince personnel to report derogatory information which may affect a coworker's continued eligibility for access to classified information.

4. Demonstrate and convince personnel that *any* unauthorized disclosure of classified information is potentially damaging to national security.

5. Make realistic the threat that anyone could be the target of a recruitment attempt, anywhere in this country.

6. Demonstrate and convince personnel that people who acquire information for foreign intelligence services are more likely to be cleared U.S. citizens than foreign intelligence agents working under cover in this country.

Interviewees were also asked to rate the difficulty of achieving each objective, using a 5-point scale graded in steps from very easy to very difficult. Responses to this portion of the survey were gathered from all but one of the interviewees.

Twenty-four interviewees felt that the single most important objective listed was ensuring that employees recognized that compliance with security rules has a positive impact on national security. While a clear majority agreed on the importance of this goal, it was ranked only moderately difficult to achieve. Twelve interviewees felt that convincing personnel to report derogatory information on coworkers was most important. This goal was rated difficult to achieve; in fact, it was considered the most difficult of the six objectives listed.

Demonstrating and convincing personnel that *any* unauthorized disclosure of classified information is potentially damaging to national security was judged the most important objective by five of the interviewees. It was rated moderately difficult to achieve. Only three interviewees indicated that the most important objective was to

convince personnel that cleared U. S. citizens are more likely to acquire information for foreign intelligence services than foreign agents working under cover. This task was considered fairly easy to achieve.

The two least-important objectives involved bringing home the threat that anyone, anywhere could be the target of a recruitment attempt, and convincing personnel that past instances of espionage have damaged national security. The former was considered moderately difficult to achieve while the latter was rated the easiest to accomplish.

Over two thirds of the interview participants responded that they had been unable to satisfy some of the objectives listed. They were then asked to identify the greatest barriers to achieving these objectives. Regarding the reporting of derogatory information, many interviewees felt that societal norms which prohibit people from "ratting" on each other prevented this objective from being reached. Personal loyalties, peer pressure, and a lack of positive motivation for informing on coworkers were all reasons that made this end so difficult. Concerning the unauthorized disclosure of classified information, several stated that overclassification of materials undermined the credibility of the system and made work towards this goal more onerous. The perceived vagueness of any threat stemming from unauthorized disclosure was also mentioned.

Two main barriers to a willing compliance with security rules and regulations were noted by some. One involved the difficulty of conveying to personnel the concept of national security and its importance. Convincing personnel that a real and credible threat to national security actually existed constituted the second problem. A few interviewees also mentioned the difficulty in convincing personnel that the information they possessed could make them possible targets of a recruitment attempt.

Coverage of Security Topics

Interviewees were asked to estimate the total amount of time each cleared person spends on SATE briefings and meetings each year. The median figure provided was 4 hours[2]. Twenty-seven interviewees felt that the time indicated was not enough, 16 declared it to be just the right amount, and no one thought it was too much.

Interviewees were then asked to estimate the percentage of time, out of the total security awareness training time, spent covering each of the following general topics: safeguarding, authorized access, accountability, espionage threat, and communications and transmission. These figures were gathered for indoctrination and refresher briefings separately. Definitions given to interviewees for these topic areas are provided in Table 2.

---

[2] It should be noted that this statistic represents the opinion of the security managers: it was not obtained directly from job incumbents.

Table 2

SATE Topic Definitions

Safeguarding - physical safeguarding of classified information.

Authorized Access - security clearances, "need to know" for access to classified information, penalties for unauthorized disclosure, reporting adverse behavior of co-workers, security violations on the job, and reporting of security violations and compromises.

Accountability - marking and designation of classified materials, protection of sensitive but unclassified information, original and derivative classification, challenging classification decisions, and requests for classified information by unauthorized persons.

Espionage Threat - the multidiscipline intelligence threat, counterintelligence awareness, reporting requirements for contacts with designated nationals, reporting requirements for anticipated foreign travel, espionage cases and lessons learned, damage to national security as a result of espionage, recruitment techniques employed by foreign agents, penalties for involvement in espionage, reporting of suspicious contacts, special vulnerabilities during foreign travel, and the terrorist threat to U.S. citizens.

Communications and Transmission - mailing of classified materials, telephone security, authorized access to classified information, and electronic transmission of classified information.

Table 3 contains the percentage of total time spent covering SATE topics in indoctrination and refresher briefings. For indoctrination briefings, the largest amount of time, 29%, was spent covering physical safeguarding of classified information. Both the espionage threat and authorized access issues consumed 20% of the time. Instruction in communications and transmission and accountability for classified materials required 16% and 15%, respectively, of the time allowed for indoctrinations. For refresher briefings, a quarter of the time, 25%, was dedicated to the espionage threat, while 24% was spent on safeguarding information. Seventeen percent of the time was devoted to each of the remaining three topics. For the two briefings, the largest amount of time was spent on the subject of safeguarding, followed by the espionage threat.

Interviewees were also asked if the time allotted for these topics was adequate, inadequate, or excessive. Generally, for both types of briefings, 75-85% of the interviewees felt that training time for the specific topics was adequate, while 15-25% felt it was inadequate. One noteworthy exception was that five respondents felt excessive attention was given to the espionage threat in refresher briefings. These interviewees, in

Table 3

Percentage of Total Time Spent Covering SATE Topics In Indoctrination and Refresher Briefings

TOPIC	INDOCTRINATION	REFRESHER
Safeguarding	29%	24%
Espionage Threat	20%	25%
Authorized Access	20%	17%
Communications and Transmission	16%	17%
Accountability	15%	17%

later remarks, mentioned that since espionage was a "sexy" topic, and had more supporting media, it got disproportionate coverage.

For topics that received insufficient time, interviewees were asked to detail the content that needed more attention. The general suggestion for all topics was that more in-depth coverage of subjects was needed. A few remarked that no area received enough attention. Only two specific areas were addressed with any frequency in interviewees' comments. In the authorized access area, a few felt that the "need to know" principle was inadequately addressed. Concerning espionage, it was suggested that the threat be made more relevant and conveyed in more realistic terms.

Reasons that contributed to the interviewees' inability to adequately cover the topics, other than lack of time, were also provided. A lack of good training design, media, and skills to get the message across was mentioned by some. It was also remarked that scheduling SATE training time was sometimes difficult because of employees' other commitments.

When asked if any of the requirements in these topic areas needed to be changed, 14 interviewees responded yes and 33 no. Those who responded affirmatively were asked to provide what they considered to be the three most important changes. Most of these specific changes were mentioned only once, but three changes were endorsed by two interviewees each. They were the need to prioritize requirements both within and across disciplines, the tailoring of Naval Investigative Service counterintelligence briefings to meet local needs and conditions, and the need to incorporate current and special topic information into SAEDA (subversion and espionage directed against U.S. Army) briefings.

Coverage of Security Disciplines

The amount of time spent preparing and delivering briefings on SATE was obtained for each of the following security disciplines: information, personnel, industrial, physical, operations, communications, and computer (AIS). Definitions for these disciplines appear in Table 4.

Table 4

Security Discipline Definitions

Information Security - The system of administrative policies and procedures for identifying, controlling and protecting from unauthorized disclosure information whose protection is authorized by executive order or statute.

Personnel Security - The processes and procedures used to ensure that acceptance and retention of personnel in the Armed forces, acceptance and retention of civilian employees in DoD, and granting members of the Armed Forces, DoD civilian employees, DoD contractors and other affiliated persons access to classified information are clearly consistent with the interests of national security.

Industrial Security - Procedures and processes for ensuring that civilian contractors doing business with U.S. government agencies follow the rules for access and safeguarding classified material entrusted to them.

Physical Security - The employment of measures to safeguard classified information, equipment or related material from loss and access or observation by unauthorized personnel.

Operations Security - The process of denying adversaries information about our capabilities and intentions by identifying, controlling and protecting information and indicators (classified or not) associated with the planning and conduct of military operations and other activities.

Communications Security - Measures taken to deny unauthorized persons information of value which could be derived through analysis of our telecommunications. Communications security is comprised of four components: cryptographic security, transmission security, emission security and physical security of communications equipment, material and documents.

Computer Security (AIS) - A specialized area of information security related to the creation and storage of classified information in individual desk-top computers, mainframe computers with remote access by individual stations and local area networks of desk-top terminals. Computer security includes risk analysis procedures and TEMPEST (compromising emanations) protection of classified computer operations.

Table 5 contains the percentage of total time spent covering the different security disciplines in indoctrination and refresher briefings. For both indoctrination and refresher briefings, the greatest amount of time, 37% and 31% respectively, was devoted to information security. The second largest slice of time for both briefings, 21%, was spent on personnel security issues. Physical, operations, communications, and computer security each consumed 10-15% of the time for both briefing types, while 2% was dedicated to the coverage of industrial security.

Table 5

Percentage of Total Time Spent Covering Security Disciplines In Indoctrination and Refresher Briefings

DISCIPLINE	INDOCTRINATION	REFRESHER
Information Security	37%	31%
Personnel Security	21%	21%
Physical Security	12%	15%
Operations Security	12%	13%
Computer Security (AIS)	10%	13%
Communications Security	10%	10%
Industrial Security	2%	2%

When comparing responses on the adequacy of coverage for the seven security disciplines, it was noted that, overall, interviewees felt that coverage of disciplines in refresher briefings was slightly less adequate than in indoctrinations. The only exception to this was physical security, where ratings of adequacy for both briefing types were very similar. For information, personnel, industrial, and physical security, 80-90% of the interviewees indicated coverage was adequate for both types of briefings, while the remaining 10-20% judged it inadequate. For operations and communications security, 74-77% felt coverage was adequate. On the other hand, a major problem was seen with coverage of computer security. In indoctrination briefings it was judged inadequate by 59% of the interviewees, and this figure climbed to 64% for refresher training.

For the disciplines that were identified as having inadequate coverage, interviewees were asked to describe what requirements needed additional attention. Nearly 80% of those responding mentioned computer security as an area requiring

considerably more time. Additional instruction in the control of data and software, including the correct handling, marking, and safeguarding of diskettes, was mentioned. Some felt that since a certain level of technological expertise was required just to understand how computers and computer networks such as LANs function, translating the vulnerabilities of automated information systems into comprehensible terms was a difficult task. Questions concerning individual accountability for information on diskettes and hard drives also needed to be addressed more thoroughly.

Regarding communications security, several stated a need for more training, focusing on the proper use and location of devices such as facsimile (FAX) machines and Secure Telephone Unit III (STU-III) telephones, and how such factors contribute to the overall security environment. A few interviewees felt that the operations security message was not getting through, perhaps because of a lack of general direction on program content and poor media support. In the area of personnel security, two responses pointed to a need for more emphasis on continuing evaluation and the reporting of derogatory information.

This lack of attention for training in the above areas was attributed to several factors, principal among them the lack of personnel and material resources. A shortage of personnel with expertise in communications and computer security was specifically noted. Rapid technological change in these areas was also considered a contributing factor. Other reasons included a lack of time and leadership support.

When asked if any of the requirements in these discipline areas needed to be changed, 22 interviewees responded yes and 25 no. Those who responded positively provided what they considered to be the most important changes. Greater emphasis and coverage of computer security was the most frequently mentioned change. This would include the use of more accessible, non-expert level language in the regulations as well as discussion of some of the security issues raised in the use of personal computers and other information systems. Additional guidance was also requested in communications security; a film summarizing the guidelines regarding the use of STU-IIIs was one example of a helpful tool. Better integration of operations security requirements, along with those of other disciplines, into the overall security environment of the command was also proposed. It was felt that the application of in-depth requirements in operations security, for example, was not always appropriate. A few also complained of a lack of specific requirements for SATE beyond holding briefings: requirements for on-the-job training and continuing education for security staff were recommended.

Training/Education Methods and Media Products

Summary

One-on-one or small-group sessions were most commonly used for indoctrination, foreign travel, special access program, and termination briefings. Larger, formal presentations were primarily reserved for counterintelligence and refresher briefings. Oral presentations almost always formed part of these educational activities, frequently accompanied by briefing aids such as overheads and reading materials. Videos and movies, guest experts, and visual reminders such as posters were employed most often in refresher and counterintelligence briefings. As a group, videotapes and movies were cited for having significant deficiencies, which included often being outdated, not very relevant, boring, and costly. The cost of posters and promotional items was also seen as prohibitive. The major deterrent to greater use of most media was their lack of availability. A centralized cataloguing and distribution system through which prospective users could become aware of and access available products was a vehicle suggested for overcoming this problem. While security officers mostly depended on their own staff and organizations for media products and services, DoDSI and security awareness groups were seen as useful and responsive in providing assistance.

Use of Training/Education Methods

A considerable portion of the survey was dedicated to ascertaining what media and training methods were employed by the security offices in SATE, where these resources came from, and how effective they were as aids in achieving SATE requirements. The first part of this inquiry focused on how requirements were currently being met. To begin, interviewees were asked to detail their use of seven different methods of dissemination in providing indoctrination, refresher, foreign travel, counterintelligence, special access program (SAP), and termination briefings (see Figure 1). Interviewee response rates differed somewhat across these briefing activities since not all were carried out in each installation. Generally, 40 or more interviewees were able to respond for all activities except counterintelligence and SAP briefings; response rates for these approached 30 and 20, respectively.

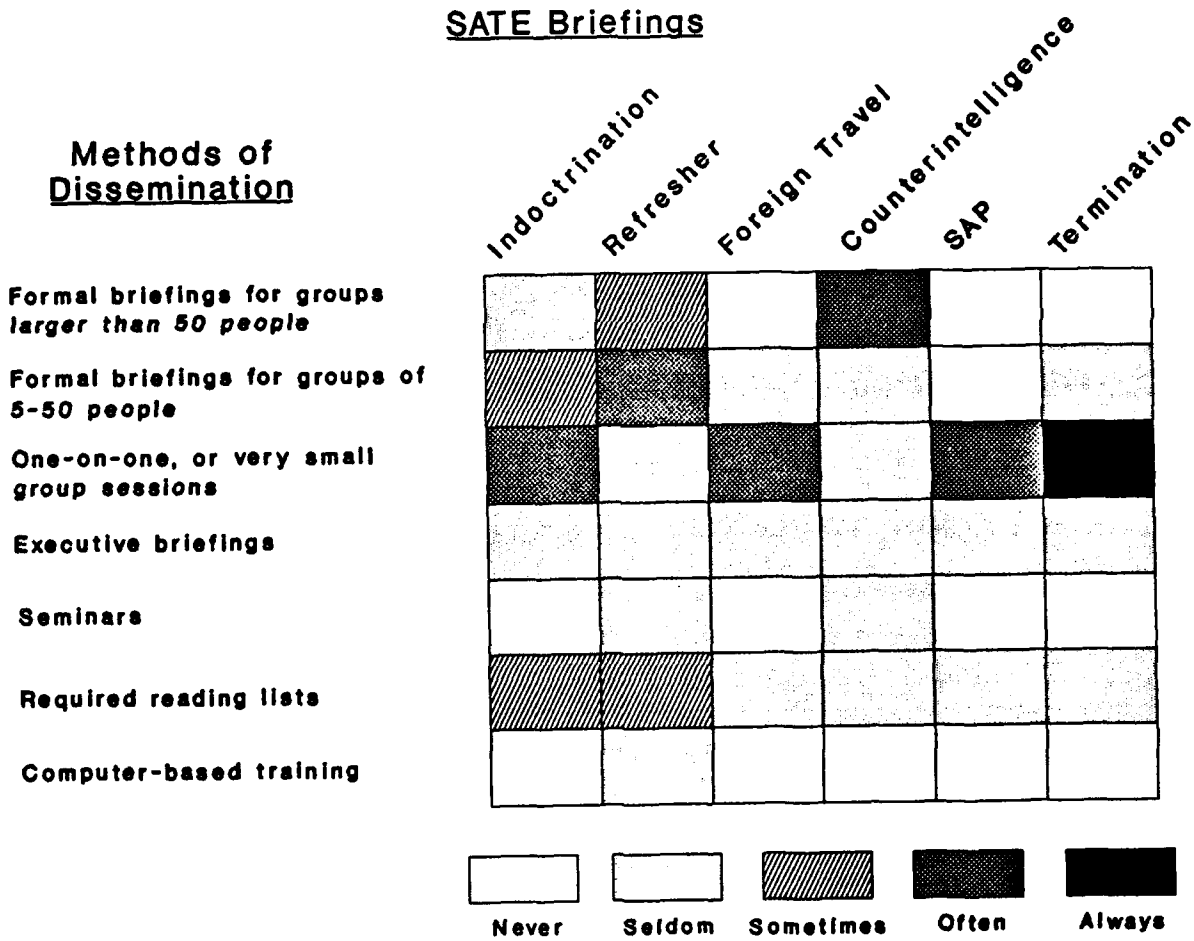
For indoctrination, foreign travel, SAP, and termination briefings, a very small group session (one-on-one or fewer than five) was most commonly used. Terminations were practically always carried out in such a setting. Counterintelligence briefings, however, were most often given in formal presentations to large groups (more than 50 people). Refresher training was sometimes given to larger audiences also, but it was most often given in stand-up briefings to groups numbering 5-50.

For the activities listed, computer-based training methods were almost never used. The use of seminars was almost as rare, and executive groups were seldom involved in the briefing activities. Required reading lists were sometimes used for training in the

same three areas, but rarely used for the other activities. Large, formal briefings were seldom used for activities other than refresher and counterintelligence briefings. Smaller, formal briefings were also used for refresher training, as well as indoctrination briefings. They were used infrequently for travel, counterintelligence, and termination briefings.

Figure 1

Usage of Different Dissemination Methods for SATE Briefings



Use of Training/Education Media

The use of 12 different types of educational media in conducting the above activities was also detailed by interviewees (see Figure 2). The individual response rate for this section was virtually the same as noted above for SATE settings. Not surprisingly, oral presentations almost always formed part of these activities. Overall, briefing aids (overheads, chalkboard, *etc.*) and systematically distributed reading material (newsletters, memos, pamphlets, *etc.*) were the two other media most frequently utilized in carrying out the activities.

Some of the media, such as computer graphics presentations, internally produced videotapes/movies, security video/movie festivals, and recorded briefings with slides, were seldom if ever used for any of the activities. Commercial videotapes/movies and promotional security items were also rarely employed, although on occasion they were used in refresher training. Guest experts and government-produced videotapes/movies were sometimes used in refresher and counterintelligence training. They were employed on an infrequent basis in indoctrination and foreign travel briefings. Posters and other visual reminders were often used for refresher training, sometimes for counterintelligence briefings and infrequently for indoctrination and foreign travel briefings.

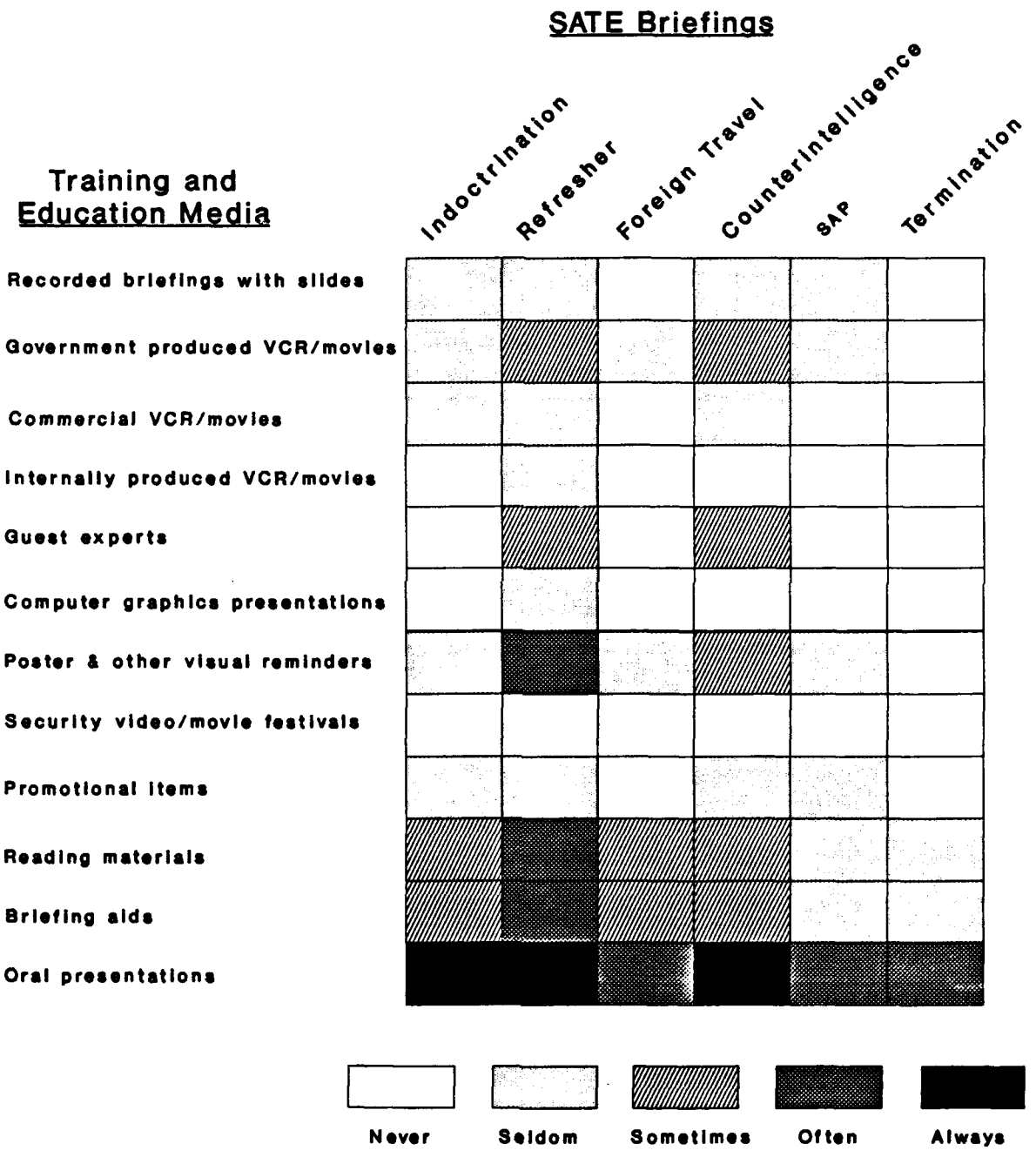
Clearly, refresher training employed the greatest variety of media on a regular basis. Counterintelligence briefings also integrated different types of media more often than other activities. Indoctrinations and foreign travel briefings primarily utilized oral presentations, briefing aids, and reading materials, but also made limited use of government-produced videotapes and visual reminders such as posters. In contrast, terminations and SAP briefings were chiefly carried out in an oral manner, and rarely employed any media other than briefing aids or written material.

Quality and Availability of Media Products

Interviewees also indicated which of the media categories had significant limitations or deficiencies, and then described those faults. The most faults were found with the videotapes and movies, as a group. Government-produced videotapes and movies were listed by 25 interviewees as having significant limitations, while 18 listed both commercial and internally produced videos as having deficiencies. The primary complaint about videos and films was their limited availability. Many interviewees did not know how to find out what might be available. These media were also criticized by several for being outdated. Cost was the third-most-common complaint. A few felt the videos were boring, aimed too low, or were not very relevant. Lack of time and money were specifically mentioned as barriers to the internal production of videos and movies.

Figure 2

Usage of Different Training and Education Media for SATE Briefings



Twenty interviewees felt that promotional items had a significant drawback; cost was the primary issue here. Computer graphics presentations and visual reminders such as posters were noted by 17 and 14, respectively, as having significant limitations. Cost was also an issue for these two media, though not as important a factor as availability.

Lack of availability was the primary complaint for all the other media. However, a fairly strong relationship appears to exist between cost and availability, according to comments. Twelve interviewees indicated that recorded briefings with slides had substantive deficiencies. A few of these criticized the medium for being boring and not allowing interaction. Only seven noted significant drawbacks with reading materials, three of those mentioning that printed materials were too long.

Very few interviewees found serious problems with the use of guest experts, security video festivals, briefing aids, or oral presentations. The only problem associated with guest experts was availability, the fundamental problem with most of the media. While one might expect that equipment compatibility for electronic media could be a major problem, very few individuals mentioned this.

Of the problems already mentioned, interviewees were then asked to list the two most important impediments to their use of the media. Once again, availability was the foremost obstacle, but often mentioned in the same breath was the lack of a cataloging and distribution system so that individuals could know what materials were out there. The cost of these items was the second most common impediment listed.

In listing the most important changes or actions that would improve the effectiveness of SATE media and products, the development of a distribution system was by far the most popular idea. Though described in many ways, its ideal form would be a DoD centralized system for cataloging and distributing SATE materials, accessible as a user-friendly database. It was felt that such a system would aid greatly in making more SATE materials available. Hand in hand with this was the call for a new and better, perhaps centralized, system of production for these media. Some interviewees commented that such a system would allow end-users to better communicate their special needs to the producers of the media.

Concerning the content of the media, several interviewees stated that improvements were needed in the overall quality, currency, and relevance of SATE products. Some of these respondents felt the establishment of the above systems would contribute to improvements in all three areas. Increased SATE funding was also endorsed by many as a necessary component for increased effectiveness. This included resources to fund the above, as well as increased time, personnel, and funds to purchase and produce SATE materials at the unit level.

Despite the comments recited above, two questionnaire items addressing both the lack of a system for cataloging and distributing SATE instructional media, and the lack of

mechanisms for publicizing their availability, were only ranked moderate problems by respondents. Lack of instructional media and materials support from headquarters was considered somewhat more of a problem than these.

Ten additional questionnaire items focused on specific problems related to SATE instructional media and materials. All but two of these items were rated moderate problems on average by respondents. Nearly 80% of respondents felt that too much specificity in instructional media was a nonexistent or minor problem. Fifty-five percent felt the same way about instructional materials being too general. The highest problem ratings pointed to a lack of SATE instructional media or materials and the tedium of existing materials; 70% considered these to be moderate to major problems. Ranked slightly below these were items concerning instructional media not being current and the lack of quality training aids and modules to assist personnel in understanding their security responsibilities. The ineffectiveness of materials in motivating individuals' security-related performance and the lack of companion instructional manuals for instructors followed closely in the ratings. The third-lowest-ranked item dealt with instructional materials being too expensive; complaints about high costs of media products, however, were frequent in the interview portion of the survey.

Sources of Media Products and Services

The extent to which interviewees relied on eight different sources for SATE products and media was also assessed. To a great extent, interviewees were dependent on themselves and their security staff for these materials. They also depended on their own organizations to some degree for SATE media and product support. They relied on DoDSI, Service headquarters, and other security managers to a lesser degree. The interviewees' reliance on security awareness groups and professional security organizations was generally negligible. They relied least on commercial vendors.

These same sources were also rated on the usefulness of their products and services and their responsiveness to requests for assistance. Only very slight differences between ratings of usefulness and responsiveness were found, so both aspects will be addressed together. As might be expected, interviewees rated themselves very highly in both areas. Mean scores well above satisfactory were given to DoDSI, security awareness groups, and their own organization. Scores for other sources were closer to a satisfactory rating, with little distinction of note between them.

Forty-one interviewees responded positively when asked if the services supplied by these sources could be improved. They also provided suggestions on how this might be done. Once again, the prevailing advice centered around establishing some sort of centralized product inventory listing and distribution system. Interviewees stated repeatedly that at present they had no way of knowing what was available. Another frequent request was for more materials and more variety in the media provided.

Improving communication between organizations involved in SATE was also mentioned, as was the need for committed resources for SATE; several security elements reported operating without a budget or designated funding level.

Accountability

Summary

Most employees received initial security indoctrination, annual refresher training, foreign travel briefings, and counterintelligence briefings as required, and attendance records for these activities were maintained at most security offices. Nevertheless, more complete coverage could be obtained through greater command attention and enforcement mechanisms. Few incentives for effective security performance were provided by commanders and supervisors, but rewards and recognition for achievement were often given at the security office level. Less than 15% of unit commanders or supervisors were themselves evaluated on security responsibilities, and a lack of penalties for poor SATE performance was noted at most levels. SATE inspections were criticized for focusing on the number of security violations and on attendance and training records rather than on measures of program quality. Improvements in the inspection process would result from spending more time, asking cleared personnel more in-depth questions, and providing greater assistance; aid in the development of a self-assessment survey based on the inspection protocol was often suggested. Program effectiveness indicators other than training records and security violations were not generally maintained, and security staffs generally relied on feedback from participants in evaluating their own programs.

Accountability for SATE Responsibilities

General questions concerning responsibilities for briefings and training and individual attendance at these functions were asked in order to ascertain the level of accountability for SATE within installations. Forty-three of those interviewed asserted that all personnel in their organization received initial security indoctrination following the granting of a security clearance. Only three indicated otherwise. When asked to provide reasons for the delay or failure to provide the initial indoctrination, administrative problems was the most common among the few responses provided.

Forty interviewees concurred with the statement that all personnel received some type of annual or periodic refresher course. The six who indicated otherwise cited temporary duty, administrative lapses, and time pressures as common reasons for personnel not receiving this training.

Similar responses were received for a question concerning special briefings for personnel anticipating foreign travel. Forty-one responded that these did take place when required by regulations or policy. Five respondents indicated they did not. Failure by personnel to report travel plans to their security manager was the most frequently

mentioned reason for missing these briefings, but time restraints imposed by short notice travel orders was also listed.

Those interviewed were also asked if records concerning individual attendance at specific briefings and training courses were maintained. For initial indoctrination, periodic refresher training, foreign travel briefings, and counterintelligence awareness training, responses were very similar; an average of 35 responded yes and 8 responded no. For termination briefings, all but four of the interviewees answered that attendance records were maintained. In response to the questionnaire item, "Attendance at SATE sessions is significantly less than desired," a majority of respondents felt this was a minor problem.

To follow up, interviewees were asked to suggest what changes or actions might be taken to ensure that all personnel receive required SATE. Two specific suggestions included tying foreign travel ticket issuance to a security briefing and distributing required materials in a pamphlet form with a roster for signatures. A recurrent general recommendation centered on commanders providing more emphasis and better enforcement mechanisms for SATE.

Four questionnaire items centered on superiors' accountability for SATE. One item which implied that installation commanders are not held accountable for security awareness was not considered a problem by a majority of respondents. Items critical of unit commanders received somewhat more endorsement. A slight majority felt that unit commanders' lack of involvement in the SATE process, along with their lack of accountability in failing to carry out SATE responsibilities, qualified as moderate problems. The supervisors' lack of accountability for the same failings was considered somewhat more of a problem.

Incentives

An attempt was made to assess what incentives, if any, were provided by personnel at different levels to reward effective security performance. Most interviewees felt that no incentives were provided by the installation commander, unit commander, or line supervisors to reward achievement in the security area. In only a few installations were letters of appreciation, citations, or pats on the back given by these individuals. At the security staff level, many more incentives and forms of praise were mentioned, the most frequent being the Security Manager of the Year Award. At relatively few of the security offices was competent performance not recognized in some way.

Numerous comments were provided on how to improve the use of incentives and rewards for promoting security awareness and performance. Poster contests with tangible rewards were endorsed by some as one of the best vehicles. Letters of appreciation from the installation commander or similar forms of command recognition were also listed as

effective ways to promote security awareness. Command emphasis and involvement was also thought to be a key to success in this endeavor.

Not surprisingly, nearly 70% of the questionnaire respondents felt that the lack of recognition for persons who are exceptionally conscientious in performing their SATE duties was a moderate to major problem. The lack of penalties for poor SATE performance also seemed to contribute to the incentives problem. The existence of few or no consequences for failing to meet SATE requirements was considered a major problem by the majority.

Security Awareness in Performance Appraisals

According to interviewees, less than 15% of unit commanders or supervisors are specifically evaluated on security responsibilities as part of their regular performance appraisal, whereas 80% of the security managers and 85% of the security staff are evaluated on the performance of their security duties.

Respondents to the questionnaire ranked the absence of personnel security issues in the performance evaluations of commanders, supervisors, and cleared personnel a moderate problem. Vague wording on the security portion of the performance evaluation form was considered somewhat less of a problem.

Security Inspections

Only one of the interviewees felt that there was too much inspection time spent in examining their SATE program, as compared to other areas of security. Twenty-two thought that just the right amount was spent, 18 felt there was too little time spent, and four claimed there was no time spent at all.

Interviewees were asked to detail some of the indicators used by inspectors in evaluating the effectiveness of their SATE activities. The two most common methods included looking for evidence that a program exists (found in documentation such as attendance records and training rosters) and the informal questioning of personnel on security procedures. Random inspections and direct tests of the system, along with the review of program reports and information on security violations, were also mentioned.

Of those interviewed, 28 believed that inspectors were more interested in the fact that a program exists than in the quality of the program. Twelve disagreed with that characterization. Of the former, the overwhelming majority felt that this attitude had a detrimental effect on the quality of their programs and encouraged emphasis on appearances rather than substance.

Nearly all of those interviewed provided suggestions on how the inspection process could be improved as a tool for increasing security awareness. Many cited the need to develop a survey or checklist with clear criteria for use in assessing the level of security awareness at a given organization. It was suggested that the present inspection protocol might be shared with security managers and adapted for this purpose. The instrument could be used as a self-assessment guide and quizzes might be derived from it to test the knowledge of installation personnel concerning security requirements. Another frequent suggestion was that inspectors spend more time asking in-depth questions of personnel, rather than focusing on program documentation and the security manager interview. A random, informal quiz of individuals on what they need to know was suggested as an excellent way of judging the overall quality of the SATE program. A few mentioned having inspectors sit in on security education briefings as being potentially useful.

The inspectors' approach in evaluating SATE was also criticized for being too punitive. Several indicated that the checklist approach should be dropped or modified, since the lists lacked sufficient detail in specific areas and encouraged "pencil whipping." A more cooperative approach, in which inspectors assisted security personnel in understanding how to meet their responsibilities, was suggested as more productive. The level of expertise among security inspectors was also questioned: it was felt that some inspectors were ill-prepared non-specialists who might be easily bluffed. Finally, some pointed out that security inspections in themselves could not improve security awareness without the proper command emphasis and support.

Questionnaire items dealing with SATE inspection issues all received minor problem rankings on average. The majority of respondents felt, in fact, that none of the following qualified as actual problems: (a) lack of SATE inspection checklists, (b) inadequate number or quality of SATE inspections, (c) SATE not included in IG inspections, and (d) SATE not included in command inspections. The last item received the lowest problem ranking by a considerable margin. At first, it may seem difficult to reconcile the low problem rankings for inspections with the abundant suggestions on how they might be improved. But when one considers that high problem rankings for the above items could be interpreted as a call for more inspections, the low rankings are not quite as anomalous.

Program Effectiveness Indicators

Questions about the types of program data and effectiveness indicators maintained by the security offices and the manner in which they are employed also formed part of the survey. The most frequently held data by far was information concerning security violations. Attendance and training records were also commonly maintained. Some interviewees remarked that reports on the results of security inspections were also held for a period of time. Security quiz results and related test scores were maintained by only a few of the security offices.

Interviewees reported several methods or indicators by which the security staff evaluate their own SATE activities. Perhaps the most frequent involved requesting informal feedback from participants in the program. This informal questioning might include asking specific questions to test the level of individual security awareness. Security violations and incidents were other frequently used measures in monitoring SATE program effectiveness. For some offices, this included analysis of reported violations to spot trends and potential weaknesses. The results of security inspections also provided some security offices with a way to gauge their effectiveness. Only three interviewees specifically mentioned having an internal inspection program in place at their installation.

From the comments elicited, it appears that two primary methods are used by installation commanders to monitor the effectiveness of their SATE activities. One is by review of the periodic security program reports which come across their desks. The other is through reports of security incidents and violations. Some installation commanders, it was reported, maintain close contact with security chiefs and receive periodic briefings. Two interviewees stated that their installation commander virtually ignored SATE activities.

Two questionnaire items addressed the general problem of how SATE programs are evaluated. The statement that SATE programs are evaluated based on the number of people trained, rather than on the quality of the program, was characterized by 70% of the respondents as a moderate to major problem. Lack of appropriate criteria for assessing the impact of SATE was judged to be a moderate problem overall. Two other items related specifically to the effectiveness of SATE procedures. Lack of knowledge regarding which aspects of the SATE program are most effective was considered overall a moderate problem, as was the absence of adequate indicators for assessing the effectiveness of SATE programs at each reporting level.

Emphasis and Support for Security Awareness

Summary

Half of the security managers stated that they did not receive adequate command support to conduct their programs, and it was felt that senior personnel did not consider SATE a top priority. More top-down emphasis on security education, beginning with OSD and reinforced at the command level, was felt necessary. Other major support problems revolved around budget deficiencies, time and personnel constraints, and lack of media support. At the Service level, quality media products and "how to" guidance on meeting requirements was especially needed. A general lack of experience among security managers was recognized, and the position was criticized for often being a part-time billet requiring much more time than available. The limited career opportunities for security personnel were also noted. The degree of emphasis placed on SATE varied directly with the nature of the command's operational mission and the types of positions within the command, rather than the security level of employees. Few differences between SATE for military and civilian personnel were identified. Security education for non-cleared personnel was generally provided, though at a lesser level.

Top Management Commitment

When interview participants were asked if they received all the necessary support to develop and implement effective SATE, the 38 responses received were evenly split down the middle; 19 yes and 19 no. Three of the most frequently mentioned support deficiencies included a lack of: (a) budget resources; (b) media support (equipment and expertise in the production of training videos, *etc.*); and most importantly, (c) consistent command emphasis and support. Suggestions were also solicited from interviewees on how the various organization echelons might provide better support for their SATE programs.

OSD. With reference to OSD, the dominant theme was that more emphasis on SATE needed to be provided from the top down. It was recommended that OSD convey to commanders and other high-ranking officials the importance of SATE, emphasizing the necessity of command support. It was also noted that in order for SATE to become a high priority, a system for providing resources and support to the program needed to be established.

Several interviewees cited the need for more instructional resources. Current, timely media with short, pithy messages applicable to a large audience were in especially short supply. A mobile SATE training and assistance team was suggested as a useful resource. A consolidated distribution system for getting SATE materials and products out, as well as a consolidated SATE resource guide, were related requests. Ensuring that security managers have the necessary training was another resource-related comment.

Some also asked for clearer and firmer requirements for SATE and better guidance on achieving SATE objectives. The establishment of "consolidated guidance for SATE, not fragmented by functional or discipline proponents," was one proposed vehicle for achieving this. One respondent asked that the "real goals" of SATE be better spelled out.

Service Headquarters. Suggestions on how the Service headquarters could better support SATE generally were similar to those provided for OSD. More command emphasis was once again a general comment, but the call for more and better media products was even stronger. The need for a security program guide with lots of "how to" information and guidance on requirements was expressed by several interviewees, as was the need for professionally produced video products tailored towards the specific Services. Some also lobbied for better distribution of existing materials and a consolidated list of SATE resources.

Several interviewees cited the need for Service-level policy changes, such as better interpretation of the DoD requirements and a consolidation of security-related requirements, with some thought given to their relative priorities. Providing training programs for security managers was mentioned fairly frequently, and better follow-up on the recommendations provided by inspectors was also listed.

Major Commands. Many of the recommendations for improved support from the major commands focused on the security manager position and his staff. Establishing security education as a full-time billet, providing more training for security managers, and giving more clout were three repeated suggestions. Understaffing of security office personnel was also a frequent complaint; a couple of interviewees complained of having their manpower "gutted." More emphasis and follow-through support from the major commander was a common recommendation, and new, improved course materials and media were again found wanting.

Installation Commanders. Interviewees had relatively fewer suggestions for improved support from installation commanders, and a few felt that no improvements were called for. The comments provided centered around devoting more personnel and funding resources to SATE and demonstrating firm personal support and interest in making a quality SATE program happen.

Unit Commanders. Suggestions for increased unit commander support generally mirrored those given for installation commanders. Again, while a few were satisfied with the support already provided, most felt that the unit commander could do more. Demonstrations of personal support for the program, such as attendance at SATE sessions and "talking up" security with subordinates, were recommended.

Related Issues. Four items from the questionnaire addressed the amount of support for SATE programs. The majority of respondents felt that the installation

commander properly emphasized SATE and that security officers had sufficient access to him or her. However, the issue of senior personnel not considering SATE a top priority was perceived as a moderate to major problem by the majority of respondents. Operational readiness priorities were also seen as adversely affecting SATE to a moderate extent.

Resources/Funding Allocated

Interviewee responses to questions about the specific resources required to fulfill their SATE requirements reinforced most of the points noted above. A lack of time, people, dollars, and media products were each listed by over 50% of the interviewees as factors which impeded their ability to carry out the SATE policies cited in OSD regulations and the DCID 1/14. Only a quarter of those responding felt that the lack of meeting facilities, networking, or AIS support impeded their effectiveness. Little more than 10% listed a lack of audio/visual equipment as a factor.

When specific resource issues were posed as problems, questionnaire responses echoed some of the concerns expressed earlier. Inadequate funding for SATE as well as the lack of a capability for producing instructional media or materials were characterized as major problems by a majority of respondents. The statement, "Security professionals lack the time or other resources required to develop high quality SATE materials," was also rated a major problem by over 50% of respondents. An item concerning the insufficient amount of training time given to covering all required SATE subjects also received a relatively high problem ranking. Nearly half felt that insufficient resources and efforts are being devoted to SATE in relation to other security functions, such as physical or information security.

Lack of equipment, such as computers and audio/visual aids, was rated a moderate concern for most respondents. Constraints which result in training sessions being too long, and lack of access to audio-visual equipment, were noted as only minor problems.

Staffing for Security Awareness Training and Education

Only three questionnaire items related specifically to staffing constraints in the security offices, and they drew quite different responses. Insufficient time for unit security managers to perform their SATE responsibilities was endorsed by over 80% of the respondents as a moderate to major problem. Sixty percent of the respondents classified understaffing in the security office in the same manner. Yet fully 70% cited an insufficient number of unit security managers as being either not a problem or only a minor one. What may appear to be an inconsistency here is merely evidence of the fact that the unit security position in generally a part-time duty. The time pressures on

security managers are well-acknowledged, but assigning additional unit security managers is not the preferred solution. In addition, less than 20% of the interviewees listed a lack of oversight as an impediment in carrying out their SATE responsibilities.

Career Field for Security Personnel

Six questionnaire items focused on problems associated with security positions or the career path available to the security professional. One item concerning inexperience among security managers and another stating that part-time managers spend too little time on SATE were considered moderate to major problems by 75% of the respondents.

Moderate problem ratings were also registered for four items that dealt with poor career opportunities for security officers and managers: (a) the low grade level for entering and senior security officers; (b) the impact of these grade levels in reducing the attractiveness of the career field; (c) failure to set minimum rank or grade levels for unit security managers; and (d) the lack of a separate, full-time position for security officers.

Program Emphasis

A considerable portion of the survey was devoted to assessing the emphasis placed on SATE by different groups within installations and finding out to which of these groups the security awareness program was most directed. The unique aspects of each installation that presented challenges for individual SATE programs also formed part of this focus on emphasis.

On average, interviewees felt that coworkers, supervisors, unit commanders, installation commanders, other commands, and non-supervisory personnel with access to classified information placed moderate emphasis on SATE. As one might expect, non-supervisory personnel without access to classified information were thought to place a low priority on SATE. Unit security managers, other security offices, and military/security police, *i.e.*, groups directly involved with the promulgation of SATE, were seen as placing moderate to high priority on SATE.

When asked how much emphasis their SATE program placed on individuals without security clearances, interviewees split most of their responses between the *less, somewhat less,* and *about the same* emphasis categories. Only four felt that *much less* emphasis was placed on this group. Given their current resources, 14 interviewees felt that SATE for personnel without security clearances should be given the same emphasis as cleared personnel; 20 felt they should be given less. The former group argued that non-cleared personnel may be exposed to inadvertent disclosures of classified information

in their routine activities. The latter group cited the lack of a need to know and the importance of focusing training resources on those who require it most.

A related question is whether the same amount of SATE effort should be directed towards those holding Secret security clearances and those with Top Secret clearances. A majority of those interviewed felt that the same amount of training was appropriate for both groups, with some differences required in the type of training. When phrased in the questionnaire as a problem of Top Secret-level individuals not receiving more SATE emphasis than Secret-level personnel, this characterization was rejected by a majority of the respondents. Concerning their own installations, 28 of 42 interviewees felt that the same level of SATE effort was directed to persons with Top Secret and Secret clearances. Where there was different emphasis, it was required because of foreign travel requirements for Top Secret billets and increased detail in certain subjects.

Independent of the differences in access levels, a majority of interviewees also felt that more SATE effort was directed to particular positions at their installations. Many positions were noted as receiving more attention, but security managers, communications personnel, nuclear weapons employees, and those with SCI clearance were most frequently mentioned. More "in-depth coverage of materials" was the overwhelming reply to the question of how the SATE procedures differed for these groups.

Differences in SATE procedures for military and civilian personnel at installations were confirmed by only six of the 42 respondents to this question. The few differences mentioned were each unique and not substantial.

When asked to focus on the unique features of their installation that influenced their SATE program emphasis, a great variety of responses were elicited. Most interviewees stated that emphasis on SATE was dependent on the operational mission of the command. Installations with an intelligence, security or nuclear-related mission claimed a greater interest in SATE. Others, whose installations operated in a more open environment, or whose facilities were geographically removed from any strategically important areas, felt these factors contributed to less emphasis being placed on SATE. One problem mentioned by several respondents concerned the effects on SATE posed by having individuals with high-level security clearances work side by side with those with lower level clearances or no clearance at all.

Interviewees were asked if the proportion of civilian to service personnel working at their installations posed unique problems or challenges. Thirty-three responded negatively, and only 7 responded yes. The few problems pointed to were generally administrative in nature.

With reference to their geographical location, only 12 interviewees felt that special problems arose with their installation's SATE program because it was located in the continental U. S. Twenty-eight respondents did not. In addition, 34 interviewees agreed

that more SATE emphasis should be directed to installations in certain geographic areas, such as overseas near hostile countries.

Peer/Subordinate Receptivity

One item from the questionnaire portion of the survey asked how serious the problem of poor attitudes toward personnel security was among installation personnel. The average ranking of this item put it somewhere between a minor and moderate problem.

Security Awareness Training and Education Regulations

Summary

In general, the DCID 1/14 and security regulations that address SATE at the DoD level (5200.1-R and 5200.2-R), the Service level, and the local level were rated as adequate. Nevertheless, respondents indicated the desirability of modifications to some service and local regulations, such as including input from users, eliminating obsolete and contradictory requirements, and providing more detail in certain subject matters. In particular, the use of clearer language and including more examples of how SATE tasks are to be completed were recommended. Virtually no conflict between SATE regulations issued at the OSD and Service level was noted, while more inconsistencies were found between Service and local regulations. Across the Services, a frequent suggestion was that all SATE guidance be consolidated in one regulation. Local rules were criticized for sometimes being out of date. SATE policy was often viewed as ensuring administrative efficiency rather than meeting an identified threat; it was also seen lacking in standardization since it came from too many sources.

Office of the Secretary of Defense (OSD)/Director Central Intelligence (DCI)

Security professionals in the DoD are often required to adhere to security regulations produced by three different groups: OSD and the DCI, the particular component under which the security unit may operate, and local entities which may also issue security guidelines.

When asked to rate the adequacy of the OSD regulations and the DCID 1/14, slightly more than half the respondents felt capable of rating the DoD 5200.1-R and the DoD 5200.2-R, but far fewer were able to rate the DCID 1/14 or the Industrial Security Manual (ISM). All ratings that were received for these regulations fell within the average to above-average range.

When asked specifically if the DCID 1/14, the 5200.1-R, or the 5200.2-R regulations needed to be improved, a much clearer difference in opinion was revealed. Only two of the interviewees responding felt that the DCID 1/14 needed to be improved. For both 5200 series regulations, half of the respondents felt there was reason to change the documents. Some of the general criticism leveled against both documents pointed to a lack of clarity, realism, and organization in some sections. The charge made by one respondent that "revisions are not adequately integrated" seems supported by other criticism that some sections are confusing and contradictory, and "include obsolete language and requirements."

Thirteen questionnaire items dealt with specific problems concerning OSD policy guidance. The item that received the highest mean ranking as a problem was: "SATE regulations are developed and issued without sufficient input from those responsible for their execution." Other items with scores in the *moderate problem* range echoed interviewees' written comments to the effect that SATE regulations are not uniformly followed, they lack sufficient detail in certain subject areas, and compliance with certain regulations is unrealistic. Two additional problems concerned the failure of SATE regulations in prescribing appropriate means for achieving security awareness and in providing consistent guidance across the military Services and civilian contractor organizations.

Items classified as *minor problems* included statements to the effect that SATE regulations are poorly organized, are not well-conceived, are too complex, lack coverage of important subjects, fail to clearly establish standards for security awareness, and are not well understood. Again, these replicate some of the comments provided by interviewees. An item which stated that SATE regulations were overly constraining and stifled individual creativity in developing security awareness received the lowest problem rating.

Service Branch

Interviewees were also asked to provide the titles of all applicable Service regulations and to rate the adequacy of these documents. Service-level regulations governing personnel and information security were most frequently mentioned, followed by regulations addressing SATE at the SCI level. After these, the most commonly used regulations dealt with, in descending order, AIS security, physical security, industrial security management, operations security, and counterintelligence education. Other less-common regulations addressed security concerns in NATO, SAEDA, and communications.

Ratings for the adequacy of these regulations also fell within the average to above average range. However, when asked if their Service SATE regulations needed improvement, 31 interviewees responded yes and only 15 responded no. When the mean

ratings by each Service were considered separately, no clear pattern of differences in rating standards emerged.

Interviewees provided a long list of improvements for their SATE regulations at the Service level. Across the Services, the most frequent suggestion was that all SATE guidance be consolidated and placed in one document. This would eliminate contradictions and repetition among regulations, facilitate updates, and make the execution of SATE generally less confusing. Another universal complaint was that regulations are too ambiguous, leaving room for differing interpretations. It was stated that more detailed, specific guidance on how to meet requirements would be a great benefit.

Some comments were directed towards specific Service regulations. For example, the Air Force 201-1 was identified by some as being particularly unclear, confusing, and difficult to follow. The Navy 5510.1H was criticized for the same reasons, but interviewees also cited the need for more and better examples, greater precision in the language used, and a reorganization of the document to make it more user-friendly. Regarding the Army regulations, it was recommended that some unrealistic requirements, especially concerning AIS, be eliminated. It was also noted that the 380.5 and the 380.67 are merely embellishments of the 5200.1-R and 5200.2-R, and that the Army might consider adapting the regulations with an eye towards meeting their own goals for SATE.

Potential problems concerning the SATE policy guidance provided by the Services were listed in the questionnaire portion of the survey. Two of these items were ranked as moderate problems. The major complaint was that Service regulations are developed and issued without sufficient input from those responsible for their execution. Also, respondents felt that Service SATE regulations fail to prescribe appropriate means for achieving security awareness. Responses to other items generally mirrored those given above for OSD-relevant problems but at a lesser level of concern. An item concerning conflicts between OSD and Service SATE regulations received the lowest ranking; nearly 50% felt it constituted no problem at all. An item which described SATE regulations as overly constraining received a similar response; over 70% felt it to be either a minor problem or no problem.

Local

An assessment of the adequacy of local SATE regulations was also made. Ratings for specific local regulations all fell within the average to above average category, as was the case with OSD and Service regulations. Some ambivalence was expressed concerning the need for improvement of these local rules, with 26 expressing a need for change and 21 seeing no need.

The most frequently expressed complaint about local regulations was their obsolescence; a need to update was expressed by many. Several interviewees found duplication in local and other directives resulting in possible conflicts. Local regulations were criticized by some for being incomplete and difficult to use. A "how to" format for these regulations which would include study guides, lesson plans, *etc.* was suggested to remedy this problem. Some felt that consolidation and reduction of the regulations would be a great benefit.

Policy Guidance/Coordination Among Components

When asked if a lack of policy guidance impeded their effectiveness in implementing the various SATE regulations, only 12 interviewees responded positively. Questionnaire items which addressed problems in general policy guidance did not elicit great variation in respondents' average rankings, with one possible exception. The statement that SATE policy seems to be based more on ensuring administrative efficiency than on meeting an identified threat was regarded as a moderate to major problem by more than 70% of those responding. Also recognized as a moderate to major problem by 60% of those responding was the assertion that SATE policy guidance comes from too many sources and lacks standardization of requirements. Yet the flip side to this is the fact that 40% felt this to be a minor or nonexistent problem. Responding to the assertion that policy provides inadequate definition of the required SATE topic areas and their associated content, most respondents judged this a moderate problem. A related item, which stated that this required SATE content does not contribute to effective security performance was viewed by the majority as a minor or nonexistent problem.

Training for Security Personnel

Summary

Security managers and their staffs felt they could benefit from additional training to enhance their general presentation and teaching skills. While they felt their SATE presentations were generally well received, they lacked skills in the design and effective use of audio-visual aids, persuasive writing, and the oral delivery of briefings. Security personnel felt most capable of carrying out their duties associated with safeguarding of classified information, authorized access, and accountability, but voiced a need for additional training in computer and communications security. Existing training courses provided by DoDSI, the Armed Services and commercial vendors were rated above average in quality but were not easily accessible.

Security Topics and Disciplines

Individuals were asked to note security topics in which they felt they had insufficient training or expertise to meet their SATE responsibilities. Most felt they were capable of carrying out their duties associated with safeguarding, authorized access, and accountability. However, the majority felt they needed more training or experience in the areas of communications and transmissions. Nearly a third also felt they lacked preparation in dealing with the espionage threat.

When asked to note specific disciplines in which they could use more training or experience, computer and communications security, respectively, were most frequently indicated. More than a third of those interviewed also felt that industrial security was a topic in which they could use additional training. Operations security and physical security were also regarded by some individuals as areas that might require more preparation. Nearly everyone felt fully able to deal with information and personnel security topics, which is not surprising since most interviewees were security officers and managers with backgrounds in these disciplines.

Overall, questionnaire respondents felt that lack of or inadequate training for security professionals in SATE requirements for different security disciplines was a moderate problem, although nearly a third felt it was a major problem.

Training/Education Methods

Interviewees were asked to assess their own skills and those of others on their security staff along seven different skill dimensions regarding the design and delivery of SATE presentations. Most mean ratings fell in the satisfactory to good range. Respondents felt that they and others were most effective in projecting their professional credibility, keeping the audience's attention and being well-received by senior audiences. They felt least-skilled in the design and effective use of audio-visual aids for presentations. The ability to bring routine materials alive was the third-lowest-ranked skill, and the design of effective training sessions fell in the middle of the average rankings.

When responding to the questionnaire items, a slight majority called inadequate SATE training for security officers and unit security managers a moderate problem. More than 40% indicated that inadequate instructional manuals or videotapes for developing SATE problems constituted a major problem. Similarly, lack of training in persuasive writing, along with inadequate training in the planning and delivery of briefings, were viewed as moderate to major problems by a majority of the questionnaire respondents.

Having already noted many of the deficiencies in SATE training for security personnel, interviewees were asked if training existed that they felt could aid them in meeting their SATE responsibilities. Thirty responded yes while 10 responded no. The former provided an extensive list of desired training topics, most of which focused on building general training skills. Many felt they especially needed help in improving their presentation skills, as well as assistance in the design and use of audiovisual materials. A "how to" course for security managers, covering all the pertinent subject areas, was strongly recommended. Security manager training is apparently available for some but not all who need it. Continuing education activities, such as periodic conferences or seminars prepared by superiors, were suggested as ways for security managers to share ideas and keep up on SATE-related developments. More training in computer and communications security was also called for. A course for the non-computer professional seemed to be especially needed.

Thirty-two interviewees responded that additional training could benefit other staff members in meeting their SATE responsibilities. Most of these recommendations duplicated those mentioned above, the most frequent being the need to develop briefing skills and effective presentation techniques. Training across the various disciplines such as computer, communications, and physical security, was also recommended by several respondents. Assistance in the design and production of media and skill development in administrative duties were also noted.

Training Sources

Interviewees were asked to evaluate training courses for their security personnel provided by external sources, including DoDSI, the Armed Services, and commercial vendors. A five-point scale ranging from very low to outstanding was used to rate the quality of instruction and course content/design, the availability, and the overall value of such programs.

All three outside training sources received above average ratings for the quality of course instruction and design. Availability, which was defined as the extent to which training at reasonable cost was easily accessible, was rated lower for all sources. Commercial and other sources received mostly above average rankings, though fewer than 10 respondents acknowledged using these sources. Courses from the Services were rated as being somewhat less available, while DoDSI services were judged lowest for availability.

In terms of the overall value of these programs--learning essential information and skills highly relevant to achieving SATE objectives would be considered valuable--most ratings fell just short of the *above average* mark. Though relatively small differences between overall source ratings were noted, the ranking from high to low was: DoDSI, Service, then commercial programs.

SATE Effectiveness

Summary

Security managers felt their programs were especially effective in establishing close personal contact with installation personnel, in providing staff assistance visits and program reviews, and in distributing security reminders and other written materials on a continuing basis. A lack of command support and management emphasis was seen as the weak link in many programs, contributing to poor briefings and apathy among personnel. After more command emphasis, the most important factors in developing an effective SATE program were a capable, motivated security staff, high visibility, and the credibility that came from leading by example and establishing oneself as a reliable source of support for security personnel. Most components of SATE programs were judged to be moderately effective, yet improvements could render most components very effective. Substantial room for improvement was especially noted in the availability of media products and services and the emphasis placed on SATE. Little room for improvement was indicated in DoD security policies or the coverage of security topics and disciplines, both which were considered to be working well.

In the final section of the interview, two different methods of inquiry were used to help in identifying the components of the SATE program that were most and least successful, and the areas in which the greatest potential for improvement existed. The first method involved asking open-ended questions and the second required interviewees to provide ratings of current and potential effectiveness for a number of specified components.

Initially, interviewees were asked to summarize which aspects of the SATE program worked best at their installations. The area most frequently cited was the close personal contact and rapport maintained by the security staff with other installation personnel. One-on-one personal involvement with employees, an open-door policy at the security office, and an expressed willingness to help were all parts of this program area which drew praise. Three other areas also received frequent mention. The first addressed the quality and usefulness of security inspection programs and reviews and the help provided in security assistance visits. The second area involved the constant reminders, memos, newsletters, and other written communications produced by the security staff to heighten security awareness. The third area concerned the quality of specific briefings; personalized, one-on-one indoctrinations were mentioned as a strong point. Two other areas mentioned somewhat less frequently were the expertise and motivation of the security staff and the training opportunities available to the security manager.

Interviewees were also asked to detail the least successful aspects of their SATE programs. A large number of comments centered on problems with specific briefing types. The indoctrination briefing was mentioned most often; it was suggested that too much information was provided for new members to absorb. A lack of command

support and management emphasis was a failing also noted with some regularity. Inadequate training for security managers and their staff was another problem sometimes mentioned.

Though noted less frequently, four other areas were also addressed by interviewees. They were poor quality and limited access to relevant media, lack of incentives for effective security performance contributing to general apathy, inadequate training in execution of AIS security procedures, and a lack of committed resources to the SATE program.

Interviewees were also asked to list the most important factor in developing an effective SATE program. Their responses addressed four different but interrelated areas, each of which was endorsed by a similar number of respondents as being the most important. A well-trained, informed, and motivated security staff seemed to form the foundation for success. Beyond this, visibility and credibility were two key factors related to an effective program for many interviewees. They were generally achieved by the same means: getting out and meeting face-to-face with customers, reinforcing security awareness in print and in person, leading by example, and establishing oneself as a reliable source of support for security managers and other personnel. Developing a support network both within and outside one's organization was specifically mentioned as a way of building towards these dual goals. The last factor, gaining command support and emphasis, was the component that could potentially contribute most to the realization of SATE goals. Being able to "sell" commanders on the importance of security seems to help immensely in the development of an effective SATE program.

Finally, the impact that current SATE programs have on the level of security awareness for five different groups was assessed. As might be expected, uncleared individuals were by far the least impacted. The level of security awareness for top leadership was moderately affected, but less so than for middle managers, supervisors, and other cleared personnel. For these last three groups, the estimated impact was rated very similar, all falling in the moderate range.

Respondents were then asked to review the 15 different SATE components listed below:

1. OSD and DCI security policies (*i.e.*, 5200.2-R; DCID 1/14)
2. Service branch SATE policies
3. Local SATE policies
4. Coverage of security topics and disciplines
5. Training/experience of personnel with SATE responsibilities
6. Media or training methods
7. Availability of media products and services
8. Usefulness of media products and services
9. Performance appraisal (related to SATE)

10. Incentives for effective security performance at this installation
11. Inspections/staff assistance visits (related to SATE)
12. Indicators of SATE program effectiveness
13. Security office staff training in SATE
14. Unit security staff training in SATE
15. Emphasis placed on security awareness

Respondents were then asked to assess the current and potential effectiveness of each in ensuring security awareness using a 10-point scale with a low ranking of *very ineffective* and a high ranking of *very effective*. For current effectiveness, all of the components received average ratings in the *moderately effective* range. Of these, the three lowest ratings concerned the availability of media products and services, SATE performance appraisals, and incentives for effective security performance. The two components ranked highest were local SATE policies and the coverage of security topics and disciplines. No clear ranking emerged for the other components whose scores placed them in the middle of the ratings.

When asked to estimate how effective various SATE components *could* be in ensuring security awareness, average ratings generally fell in the *very effective* range. The component with the most potential for ensuring security objectives was identified as the emphasis placed on security awareness. Other components such as the training/experience of personnel with SATE responsibilities, local SATE policies, and media or training methods also received relatively higher ratings for potential effectiveness. The lowest potential was seen for SATE-related performance appraisals and incentives for effective security performance.

The difference between the mean ratings of potential and current effectiveness were calculated to determine how much interviewees felt each component could be improved. The availability of media products and services was the area in which the most room for improvement was noted; respondents' average scores indicated that effectiveness in that area could be nearly doubled. Other areas with room for improvement included unit security staff training in SATE and the emphasis placed on security awareness. Components in which the least potential for increased effectiveness existed were DoD security policies and coverage of security topics and disciplines; they were considered effective in their present state.

Respondents were also asked to evaluate their own SATE programs. Overall, they rated their current programs as moderately effective. While several raters considered their programs very effective, relatively few classified them as ineffective.

Other Survey Topics

Three questionnaire items centered on subjects that did not easily fit into any of the above headings. One item concerned rapid turnover in the cleared population and the other stated that SATE programs of the Services differ and should be consolidated into a single program. Both of them were rated as moderate problems, on average, though the majority of responses for these items fell in the *not a problem* or *minor problem* categories. The final item, having some units on the installation not covered by the installation SATE program, was rated a very minor problem.

IMPLICATIONS OF FINDINGS AND RECOMMENDATIONS

This section discusses implications of the survey findings for SATE policy and programs and provides recommendations for improvement. It should be noted that overall, security managers rated their SATE programs as moderately successful. They felt that they had provided personnel with the required security indoctrinations and had positively contributed to the security inspection and review process.

In the process of reviewing survey results, five major problem areas or themes were identified, some which cut across the eight content areas reviewed in the previous section. It is in these specific areas where additional assistance to the security manager could result in the greatest improvements to SATE programs. They are instructional media enhancements, security manager training, SATE policy and requirements, security manager support, and security inspections.

Two of these, instructional media enhancements and security manager training, would have the greatest impact and are addressed below under primary implications and recommendations. Improvements to SATE policy and requirements, increased security manager support, and improved inspections are seen as having important but lesser impact, and are listed under secondary implications and recommendations.

Primary Implications and Recommendations

Instructional Media Enhancements

Issues. Security professionals repeatedly expressed concern with the availability and quality of media products. Many had virtually no access to information concerning what materials might be available and how to procure them. In addition, cost frequently prohibited them from obtaining some of the products. Lack of a reliable, timely, and sufficiently comprehensive distribution system also prevented them from acquiring more commonly available SATE publications and materials.

Of the media products used in security education, much of the criticism was reserved for videotapes and movies. They were frequently faulted for their lack of relevance to local security conditions, for being out of date, and for being boring. Security managers expressed frustration in not having the available resources to develop media to meet their own specific needs.

Recommendations. Provide better security materials in a timely fashion to security managers. There are two components to this recommendation.

1. Improve the distribution of SATE materials. Consider creating a centralized distribution system for materials that would be easily accessible to security managers. This would entail establishing an office responsible for acquiring and disseminating security materials. The office could serve as a clearinghouse for SATE materials produced at DoD, Service headquarters, or at the local level. It could also function to coordinate acquisition of training aids across organizations; provide guidance in the development and utilization of materials; and facilitate professional networking for the exchange of ideas, media products and assistance. DoDSI has, in fact, recently established a security awareness products clearinghouse and is currently soliciting materials for evaluation and possible inclusion in their products catalog.

2. Improve the quality of materials developed at DoD and Service headquarters levels. Additional assistance could be given to the field by improving materials such as security posters, videotapes, pamphlets and newsletters. Explore the feasibility of using computer-based approaches, such as instructional modules, adventure games and on-screen security reminders. The above-mentioned clearinghouse could provide guidance in design and distribution of the media products and in assessing their utility.

Security Manager Training

Issues. Newly assigned security managers lack appropriate experience or training in their positions. Deficiencies are due, in part, to the nature of the career path for security managers. It provides limited opportunity for developing the knowledge and skills required to design and implement effective SATE. Also, opportunities to attend training courses on the job are very limited (Bosshardt, DuBois & Crawford, 1991c). Training opportunities are not readily accessible due to their location, limited class sizes and time requirements. Shortcomings attributed to inadequate training included a lack of expertise in creating media products, in preparing and delivering briefings, in clearly articulating security threats, and in instructing personnel in technologically sophisticated areas such as computer and communications security.

Recommendations. Bring training to the security manager rather than requiring the manager to attend formal courses at another location. Two ways to achieve this would be:

1. Develop a correspondence course for new security staff. The course could be developed around a generic DoD core of information and contain additional modules for Service-specific requirements. Particular attention should be paid to the rapidly emerging security needs in the computer and communications areas. In this regard, DoDSI is currently developing a series of correspondence subcourses for the DoD security professional. Completion of these correspondence modules will be required prior to attendance at the DoD Security Specialist Course. A correspondence course in Personnel Security Administration and Management is also being planned.

2. Conduct training at regional locations where requirements for travel to training could be minimized. Regional resources, such as counterintelligence professionals, could be employed to improve the quality and relevance of SATE. Another possibility for more accessible training would be through the increased use of mobile SATE training teams.

Secondary Implications and Recommendations

SATE Policy and Requirements

Issues. Some of the problems associated with SATE at the installation/unit level arise from the existence of multiple Service and local regulations in which requirements for security education in various disciplines are presented separately. Security managers reported finding the same requirement repeated in different regulations, having to reconcile contradictory requirements, having to deal with obsolete requirements and poorly integrated updates, and having difficulty determining the relative priority of diverse requirements. The inadequate organization of many regulations also made it difficult to locate all the requirements relating to security education in a given subject area. Interviewees decried the lack of specific guidance--beyond a statement of required briefings--in how to meet SATE objectives. Computer and communications security regulations were frequently singled out as difficult to use because the language which was employed presupposed a level of technological knowledge that many security personnel did not possess.

Recommendations. In general, regulations should be made easier to use and material relevant to a particular issue should be located in a single section or, at a minimum, cross-referenced for ease of use.

1. Consideration should be given to simplifying and/or reducing the number of regulations and supplements. Contradictions and repetition among regulations should be eliminated. This effort should be initiated at the DoD level, perhaps as a special task group made up of OSD, Service headquarters and field representatives.

2. Guidance should be provided and procedures should be established for improving the translation of Service SATE regulations into local regulations.

Security Manager Support

Issues. Command support and emphasis was seen as essential by security managers but non-existent for half of those interviewed. In particular, few commanders or others in top leadership were visible in security awareness training activities, nor did

they provide effective mechanisms for enabling the security manager to enforce compliance with security requirements. In addition, as might be expected, security offices perceived a shortage of budgetary and personnel resources provided by the command.

Recommendations. The recommendations address means for assisting the security manager within existing budgetary constraints.

1. Provide senior officers and management with indoctrination and continuing reminders of the role and importance of SATE to their organization's security. One possibility would be to provide security awareness training in officers' professional education and in ongoing training courses for all leadership levels.

2. Structure SATE programs to involve commanders and senior staff. One possibility would be greater personal involvement in security indoctrinations. Another would be greater attention to the allocation of security resources and to reallocation where needed.

Inspections

Issues. Security managers felt that the inspections did not contribute to SATE program effectiveness. They commented that inspections focus on documenting compliance with briefing requirements (reports of security violations and training attendance records) rather than on the impact of programs on the cleared population.

Recommendations.

1. Better tools or instruments are needed for assessing the effectiveness of SATE programs at the unit and installation levels. These tools could be employed by security managers for self-appraisal and during inspections.

2. Security inspections could profit by evaluating the impact of SATE on cleared personnel. More systematic interviewing or evaluation of supervisors, unit commanders and cleared individuals could be employed. Security managers would benefit from assistance-oriented inspections where inspectors provide helpful feedback during and after inspections.

Additional Support For Survey Recommendations

The above five sets of recommendations resulting from the survey are supported by recommendations provided by participants in the initial headquarters and field site visits, by the recommendations of an earlier related study, and by findings contained in two DoD reports and two Congressional reports.

Approximately 40 recommendations for improving SATE programs resulted from discussions with headquarters officials in the initial phase of the project. Nearly all of these recommendations fell into the areas of instructional media enhancements, security manager training, and security manager support. They included making SATE instructional materials more accessible, identifying better methods for presenting SATE, improving the competency of security professionals in performing their SATE responsibilities, and increasing commander and supervisor support and accountability for SATE.

The initial field site interviews also resulted in over 40 ideas for improving SATE. Recommendations addressed all five of the areas identified above with the exception of security manager support. Suggested improvements included providing mechanisms for communication among security staff across Service branches, providing professionally developed training packages, making professional training more accessible, integrating SATE regulations across security disciplines, and developing program evaluation tools.

Virtually all of the recommended actions found in this report are contained, in similar form, in a study on continuing assessment of personnel in the military (Bosshardt, DuBois, and Crawford, 1991b). While the recommendations in the Bosshardt study are directed towards improving the effectiveness of continuing assessment programs--a related but much more narrow area than SATE--many of the recommended actions are nearly identical to those found in this report.

Additional support for our recommendations comes from the findings and conclusions reached in DoD and Congressional reports already mentioned and from a report to the President on the National Industrial Security Program (NISP) (Secretary of Defense, 1991).

In the Stilwell Report (DoD Security Review Commission, 1985) the lack of a central distribution system for security-related information and publications was noted and it was suggested that establishment of such a clearinghouse program would result in great benefit. In the area of security manager training, the report recommended the establishment of "minimal levels of required training for DoD military and civilian personnel who perform security duties" (p. 89). The lack of commander and supervisor interest and involvement in security education was also noted, and the report stressed the responsibility of "commanders and supervisors to underscore the importance of the security function by personal example" (p. 14).

A 1986 report (United States Senate) provided the following statement in relation to security manager training:

> One of the common themes in all recent studies of security countermeasures--the Information Security Oversight Office (ISOO) task force, the Stilwell Commission, and the Inman Panel--is the need for better

training not only for security professionals, but also for managers and other officials having security responsibilities (p. 93).

The report suggested that "Consideration should also be given to forming under DSI an interagency group, with counterintelligence agency participation, to develop and review effective security awareness educational material and techniques" (p. 94). This report's first recommendation under instructional media enhancements provides similar advice.

A second Congressional report (United States House of Representatives, 1988) supports our recommendations on security manager training by noting that the "offices of security. . . . invite disdain because of inadequate personnel training." Its finding that "personnel and information security continue to receive less attention than other security disciplines . . " and ". . continue to go begging" certainly points to the value of a re-examination of resource allocation, as suggested in this report's recommendations under security manager support.

More recently, the NISP task force (Secretary of Defense, 1991) has drafted policy for the National Industrial Security Program Operating Manual (NISPOM) which includes "training and certification programs for both government and industry" (p. 30), underscoring once again the critical nature of adequate training for security professionals.

In all, we find DoD and Congressional reports supporting recommendations in three of our five major areas, and support for action in all areas coming from a separate study and from a series of interviews conducted in conjunction with the current study. Evidence of the need for action in the most deficient areas identified seems compelling.

REFERENCES

Bosshardt, M. J., DuBois, D. A., & Crawford, K. S. (1991a). *Continuing assessment of cleared personnel in the miliary services: Report 2 - Methodology, analysis, and results.* (Technical Report PERS-TR-91-002). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M. J., DuBois, D. A., & Crawford, K. S. (1991b). *Continuing assessment of cleared personnel in the miliary services: Report 3 - Recommendations.* (Technical Report PERS-TR-91-003). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M. J., DuBois, D. A., & Crawford, K. S. (1991c). *Continuing assessment of cleared personnel in the miliary services: Report 4 - System issues and program effectiveness.* (Technical Report PERS-TR-91-004). Monterey, CA: Defense Personnel Security Research and Education Center.

Department of Defense. (January, 1987). *Department of Defense personnel security program regulation* (DoD 5200.2-R). Washington, DC: Office of Deputy Under Secretary of Defense for Policy.

Director of Central Intelligence. (January, 1992). *Minimum personnel security standards and procedures governing eligibility for access to sensitive compartmental information* (Directive No. 1/14). Washington, DC: Author.

DoD Security Review Commission. (1985). *Keeping the nation's secrets: A report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices.* Washington, DC: Office of the Secretary of Defense.

Secretary of Defense. (September, 1991) *The National Industrial Security Program: A report to the President.* Washington, DC: Office of the Secretary of Defense.

United States House of Representatives. (1988). *U.S. counterintelligence and security concerns: A status report. Personnel and information security.* Report submitted by the Subcommittee on Oversight and Evaluations of the Permanent Select Committee on Intelligence. Washington, DC: U. S. Government Printing Office.

United States Senate. (1986). *Meeting the espionage challenge: A review of United States counterintelligence and security programs* (Report 99-522). Report submitted by the Select Committee on Intelligence, 99th Congress, 2nd Session. Washington, DC: U. S. Government Printing Office.

LIST OF APPENDICES

APPENDIX A

DoD Requirements Regarding SATE

APPENDIX A

DoD Requirements Regarding SATE

Security awareness training and education is driven by requirements principally found in regulations governing broader activities in the DoD and defense industry, such as personnel and information security. The requirements system which guides personnel and information security, along with many other aspects of government, flows down from presidential directives and executive orders to agency or departmental regulations. Presidential directives come in two forms: the often classified National Security Decision Directives, and unclassified executive orders. Information and personnel security at collateral (Confidential, Secret and Top Secret) and sensitive compartmented information (SCI) access levels are general regulated by two different groups of requirements.

SATE Requirements For Collateral Clearances

Various administrations have issued executive orders concerning the protection of national security information at the collateral clearance level and the security education which should form part of that program. These orders deal with the classifying and safeguarding of classified information and with implementation of their provisions. The most recent of such orders was Executive Order 12356 of April 1982.

This Order set out general responsibilities for agencies that originate or handle classified information. Among such responsibilities was the requirement that agencies "designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order" (p. 14882).

In June 1982, the Information Security Oversight Office (ISOO) published detailed guidance to help agencies in carrying out Executive Order 12356. This document was entitled, *Directive No. 1 National Security Information*. A paragraph on security education appeared in Subpart E of the ISOO document. The paragraph read:

> Each agency that creates or handles national security information is required under the Order to establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings (p. 27842).

In 1985, an unclassified National Security Decision Directive, NSDD 197, was issued requiring all U. S. Government departments or agencies to implement a formalized security awareness program, which was to include "a periodic formal briefing of the threat posed by hostile intelligence services." The DoD Directive 5240.6 implemented NSDD 197 in 1986, and detailed some of the content and reporting requirements associated with the briefings.

In response to Presidential orders and directives previous to Executive Order 12356, such as the 1953 Executive Order 10450, *Security Requirements for Government Employment*, the Office of the Secretary of Defense had produced separate regulations covering information and personnel security for individuals with collateral clearances. The ISOO and National Security Decision Directives were implemented in later versions of these OSD regulations. Each regulation includes a chapter or section on security education, and lists several requirements. The latest versions of the regulations are: *5200.1-R Information Security Program Regulation*, June 1986; and *5200.2-R Personnel Security Program Regulation*, January 1987. Both documents are currently being revised.

It should be noted that separate DoD regulations governing physical security, operations security, communications security, and automated information systems (AIS) security also exist. Each regulation mandates security education training in the corresponding discipline, but the development of specific requirements is left to the heads of DoD components. Only in the information and personnel security regulations are the general form and required elements of the security education program as a whole described in substantive detail.

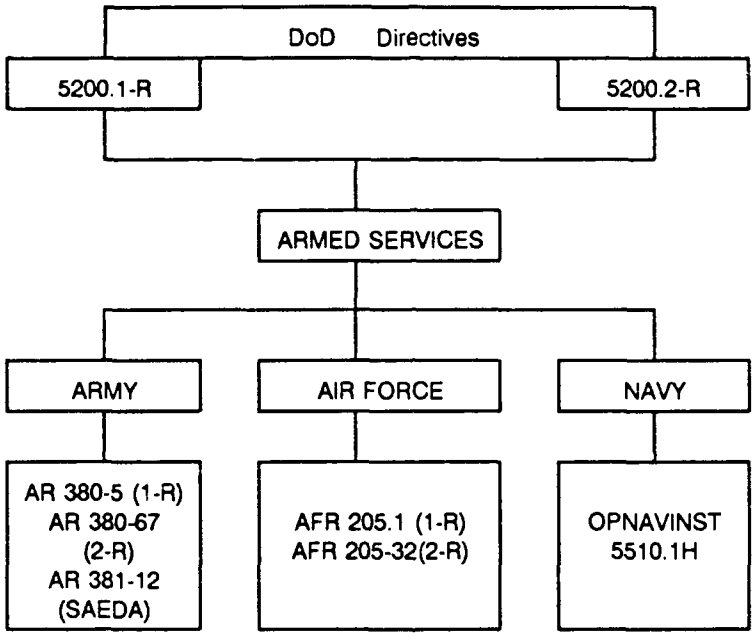
The two DoD regulations which govern personnel and information security education for individuals with collateral clearances are similar in both content and format. Both regulations introduce the subject of security education and specify four required briefings: initial, refresher, foreign travel, and termination briefings. The 5200.1-R, since it appeared earlier, was the model for the 5200.2-R and much of the same text found in the former, with slight variation, appears in the latter.

The principal way in which the two documents differ on security education is that the 5200.1-R provides general objectives and specific goals for the security education program in two sections: *Responsibility and Objectives* and *Scope and Principals*. No such statement of overall goals or purpose exists in the 5200.2-R, and the reader is at times referred back to the 5200.1-R for guidance on objectives. The 5200.2-R does provide additional clauses concerning administrative procedures to be followed in carrying out some briefings.

In implementing these two regulations at the Service level, the Army and Air Force have each produced two sets of regulations which mirror the 5200.1-R and 5200.2-R on security education, while the Navy has produced a single document which covers both the personnel and information security aspects of security education (see

Figure 1). The Army AR-380-67 and Air Force 205-32 are both descended from the 5200.2-R and their sections on security education are virtual recitations of that document, with some Service-specific additions such as references to documents, procedures, and record-keeping requirements.

FIGURE 1
DoD Directives and Armed Services Regulations
Requiring Security Awareness Education for Individuals with Collateral Clearances



Both the Army and Air Force adaptations of the 5200.1-R give additional guidance concerning the purpose of security education in general, and the goals of some briefings, in particular. These documents also direct the reader to other pertinent regulations, assign responsibility for the completion of specific tasks, list additional briefing requirements under certain circumstances, and provide additional instruction on matters such as record-keeping. Army regulation 381-12 also requires that personnel be briefed on subversion and espionage directed against U. S. Army (SAEDA) on an annual basis.

The Navy's 5510.1H integrates both the 5200.1-R and 5200.2-R requirements in its chapter on security education. A paragraph concerning the purpose of the security program is included and additional on-the-job training requirements are incorporated. Among the Services, this document provides perhaps the most detailed guidance on

meeting the security education requirements, even providing a section for security managers on how to develop a command security education program.

In summary, separate DoD directives regulate information and personnel security education, as well as training in other disciplines, for individuals with collateral clearances. The 5200.1-R, however, is often the document of greatest relevance to the security education program.

Sate Requirements for SCI Access

The most recent executive order governing the activities of the intelligence community and its classified activities, Number 12333, is dated December 1981 and is entitled *United States Intelligence Activities*. Responding to an earlier version of Executive Order 12333 (President Ford's *United States Foreign Intelligence Activities* of February 1976), the Director of Central Intelligence (DCI) issued in 1976 a security standards regulation concerning personnel with access to SCI. This regulation is the DCID 1/14 (unclassified), *Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*. The current version is dated January 1992, and the section concerning security education is Annex C, *Minimum Standards for SCI Security Awareness Programs in the U.S. Intelligence Community*.

SCI security education policy and regulations are difficult to discuss in an unclassified report because most Service and agency implementations of the DCID 1/14 are classified. Annex C of the DCID 1/14 describes a 3-part program for briefings: initial indoctrination, periodic awareness enhancement, and debriefing. Foreign travel and counterintelligence briefings fall under the periodic awareness enhancement portion of the program. The objectives and some of the content for these activities are specified, along with some of the different media that may be employed in carrying out a continuing security awareness program.

The only unclassified Service implementation of the DCID 1/14 is the Air Force regulation 201-1. Chapter 19 of this document, "Security Education/Awareness and Training," also implements portions of DoD Directive 5105.21 (M-1), which is classified. The Air Force 201-1 focusses on the specific responsibilities of personnel at different organizational levels in providing security education. The content and frequency of the various courses and briefings is detailed, and considerable direction concerning the shape and administration of the program is provided. Information and sources for developing local SCI security education are even noted.

Supplemental Guidance

In addition to the cascading regulations already mentioned, local regulations concerning security education in the form of training manuals, pamphlets, supplements, handbooks, *etc.* also form an important part of the security program at many installations. These materials may provide the security staff with the most detailed information on their SATE responsibilities. They add to the number of documents with which security managers must be familiar in order to provide an effective and conforming security program.

Overall, the Service and agency requirements for security education at both the collateral and SCI clearance levels are similar and primarily consist of five different types of briefings: initial, refresher, foreign travel, counterintelligence, and termination. Since the counterintelligence briefing was mandated only recently, it may not be specifically mentioned in all the regulations cited. Special briefings for unusual circumstances are also provided for in most regulations. Also, the objectives and goals expressed for security education in the above documents for both clearance levels are similar, though they may not be actually stated for each briefing or activity.

APPENDIX B

List of Sites Participating in Survey

APPENDIX B

List of Sites Participating in Survey

ARMY

CG WESTCOM
ATTN: APIN-SC
Ft. Shafter, HI 96858-5100

Commander, Fort George G. Meade
ATTN: AFKA-21-PTS-1
Ft. Meade, MD 20755-5090

Commander, 1st U.S. Army
ATTN: AFKA-OP-IS
Ft. George G. Meade, MD 20755-7300

Headquarters, Training & Doctrine Command, U.S. Army
ATTN: ATBO-JC
Ft. Monroe, VA 23651-5000

CECOM Center for Night Vision and Electro-optics
AMSEL-RD-NV-AOD
Fort Belvoir, VA 22060-5677

HQ U.S. CINCPAC
P.O. Box 10
Camp Smith
Honolulu, HI 96861-5025

U.S. Army Garrison
Fort Detrick
Frederick, MD 21701-5000

U.S. Army Forces Command
HQ Forces Command
FC J-2-CIN
Ft. McPherson, GA 30330-6000

Commander, U.S. Army Garrison
ATTN: AFZK-SEC
Ft. McPherson, GA 30330-5000

U.S. Army Garrison
Commander, U.S. Army Missile Command
ATTN: AMSMI-SI
Redstone Arsenal, AL 35898

Military Police & Chemical Schools
Ft. McClellan, AL 36205

Commander, U.S. Army Health Services
ATTN: HSOP/HSI
Ft. Sam Houston, TX 78234-6000

HQ 97th ARCOM
Bldg. 1250
Ft. George G. Meade, MD 20755-5340

97th ARCOM, 2122d U.S. Army Garrison
5515 Liberty Hts. Ave.
Baltimore, MD 20207

338th MIBN, 97th ARCOM
USARC, Bldg. 1251
Ft. George G. Meade, 20755-5340

7th Infantry Division and Fort Ord
ATTN: AFZW-05
Fort Ord, CA 93941-5220

Sierra Army Depot
SDSSI-CIB
Herlong, CA 96113-5192

SIAD/DSW
Sierra Army Depot

NAVY

COSC
Norfolk, VA 23511

Naval Technical Training Center
NTTC Corry Station
Pensacola, FL 32511

NSG
Washington, DC 20393

Naval Communication Station
San Diego, CA

FICPAC
CINCPACFLT
Pearl Harbor, HI 96860

USS Whipple
FPO San Francisco, CA 96683-5000

Fleet Training Group, Pearl Harbor
Pearl Harbor, HI 96860-7600

Naval Shipyard
Naval Station, Pearl Harbor
(Code 1700)
Pearl Harbor, HI 96860-5350

USS Tunny
FPO San Francisco, CA 96678

COMSUBPAC (Code 0021)
U.S. PAC Fleet
NS Pearl Harbor, HI 96860-6500

Commander Officer
VQ3
Fleet Air RECON S43
NAS, Barbers Point, HI 96862

Naval Security Group Department
Naval Radio Receiving Facility
Imperial Beach, CA 92032

MARINE CORPS

HQ U.S. Marine Corps
CODE ARF
Washington, DC 20380

Fleet Marine Force, Pacific
Camp H. M. Smith, HI 96861-5001

Marine Corps Combat Development
Command
Quantico, VA 22134-5001

HQ & Service Co.
1st MEB
MCAS, Kaneohe, HI 96863-5501

AIR FORCE

HQ TAC/INS
Langley AFB, VA 23665

TAC/SPI
Langley AFB, VA 23665

Air Training Command
Chief, Personnel & Industrial Security
HQ ATC/SPI
Randolph AFB, TX 78159-5001

Air University
3800 Air Base Wing, SPAI
Maxwell AFB, AL 36061

Electronic Security Command
Kelly AFB
HQ ESC/SPIB
San Antonio, TX 78243-5000

AFEWC/RMD
San Antonio, TX 78243

AFCSC/XRR
San Antonio, TX 78243-5000

HQ MAC/SPI
Scott AFB, IL 62225-5001

375 CSG/SPAS
Scott AFB, IL 62225-5215

AFAA/AAO
Wright-Patterson AFB, OH 45433

ASD/SPIS
Wright-Patterson AFB, OH 45433

ASD
Wright-Patterson AFB, OH

HQ AFLC/SPI
Wright-Patterson AFB, OH 45423

2750 SPS
Wright-Patterson AFB, OH 45423

HQ 15th AF/SP
March AFB, CA 92518

HQ SAC/OSP
Offutt AFB, NE 68113

SAC/LG

SAC/SPI

SAC/Unknown

SAC/ACEA

SAC/XR

SAC/XOE

930 SPS
Castle AFB
Merced, CA 95342

DOD

Armed Forces Medical Intelligence
Center
ATTN: AFMIC-RM
Fort Detrick
Frederick, MD 20702-5004